Procure Sharing Of Health Records In Cloud Using Attribute Based Encryption

T. Raj Kumar[1] G. Charles Babu[2]

[#1]*pursuing M.TECH (CSE) from Holy Mary Institute of Technology and Science, Keesara, Hyderabad, Affiliated to JNTU, Hyderabad, Andhra Pradesh, India*

[2]*working as Professor and Head of CSE Department in Holy Mary Institute of Technology and Science, Keesara, Hyderabad Affiliated to JNTU Hyderabad, Andhra Pradesh, India*

***Abstract*-Personal health record is an dynamic thinking for the allocate the health record information to one another to get the instant idea about the problem, but with that proposal numbers of issues is there in which the main concern is security of data from the un-authenticated users and hackers. In recent days it is common to hack data stolen data from the hackers or un-authenticated user. To overcome from this problem, in proposed system is, we use cryptographic method to encrypt the information, in cryptography the plain text is changed into chipper text and generate key for the use of user to decrypt that data for use. The algorithm which we are used in this paper is known as ABE (Attribute Based Encryption), the encryption is based on data attribute, on the basis of condition the encryption is working. In this algorithm the file will be encrypted under up to its attribute and key generation for decrypt the data for the usage of readable file, the public key is send to the users who are registered for share the data on its requirement.**

INTRODUCTION

Modern advances in an IT sector have mostly facilitated remote information storage and allocating. New applications such as online social networks and online documents provide very convenient ways for people to store and share various data including personal profile, electronic documents and etc on remote online data servers. PHR, regarded as the future IT architecture, and more promises to provide extended and elastic storage resource (and other computing resources) as a service to cloud users in a very cost-effective way Although still at its early stage, PHR has already get high consideration, and also its gains have attracted an increasing number of users to outsource their local data centers to remote cloud servers. Data security is a critical issue for remote data storage.

On one hand, disclosure of tricky data, such as health records, stored on remote data servers has to be strictly protected before users have liberty to use the information services such as, Fine-grained information accessing control mechanisms often need to be in place to assure appropriate disclosure of tricky data among multiple users. On the other hand, in remote data storage users do not physically possess their data. Remote data/information service providers are almost certain to be outside the users' trust domain, and are not grant to learn users' tricky information stored on their servers. It turns out that users cannot rely on remote data servers to enforce access control policies like traditional access control in which reference monitors should be totally combined. User enforced data access control is thus highly desired for remote data storage. More generally, such an issue also already exists in any un-trusted storage, e.g., In distributed data storage in Wireless Sensor Networks for which storage devices that are either owned by untrustworthy provider(s) or highly vulnerable to memory breach attacks, This dissertation addresses the issue of securing data sharing on un-trusted storage by exploring cryptographic methods to help users enforce data access policies – only encrypted data are stored on storage servers while retaining secret key(s) to the data owner herself; user access is granted by issuing the corresponding data decryption keys. In particular, we study a novel public-key cryptography – Attribute-Based Encryption (ABE), and enhance it toward providing a full-fledged cryptographic basis for a secure data sharing scheme on un-trusted storage. Based on ABE, we also present our solutions for securing data sharing in PHR

In un-trusted storage data servers are not grant to learn the content of tricky data, nor can they be relied on to enforce data access policies. To keep data confidential to data servers the data owner encrypts data before stored. Access is granted to user by possessing the data decryption key(s). When this kind of cryptographic based access control scheme provide security protection on data, there are also several major challenges apply to the scheme design. We can summarize the 2 challenges as follows.

ATTRIBUTE-BASED ENCRYPTION

We popularized the public-key cryptography attribute based encryption (ABE) for cryptographically required access control in (attribute based encryption) ABE both the user secret key and the cipher text are combined with a set of condition. A user is able to decrypt the cipher text if and only if at least a threshold number of condition overlaps between the cipher text and user secret key information. Disparate from traditional public key cryptography such as Identity-Based Encryption, ABE is intended for one-to many encryptions in which cipher texts are not necessarily encrypted to one

specific user. In sahai and Waters (attribute based encryption) ABE scheme, the limit semantics are not very energetic to be used for designing more general access control system. To enable more general access control, they proposed a key-policy attribute-based encryption (KP-ABE) scheme –a defined as ABE. The concept of a KP-ABE scheme is as follows: the cipher text is associated with a set of condition and each user secret key is embedded with an access structure which can be any monotonic tree- access structure. A user is able to decrypt a cipher text if and only if the cipher text condition satisfies the access structure embedded in his/her secret key information. In same work, Goyal et al. proposed the concept of another derived of ABE – cipher text policy attribute-based encryption (CP-ABE). CP-ABE works in the reverse way of KP-ABE in the sense that in CP-ABE the cipher text is associated with an access structure and each user secret key is embedded with a set of condition.

We identify three directions for future work for secure data sharing on un-trusted storage as follows. Decentralized Access Control In this dissertation, there is one cryptosystem in each data application and the data owner acts as the only authority in every cryptosystem. Users should possess a separate set of secret keys for each crypto encryption system. In high range systems, it is desirable to provide decentralized access control in the sense that on one hand we enable users to access multiple cryptosystems using one set of secret keys, and on the other hand we allow the existence of multiple authorities in an application as well as encryption of data using public keys assigned by multiple authorities. The concept of decentralized ABE provides the cryptographic basis for this feature. Anyhow, existing mechanisms for decentralized ABE have various limitations in terms of the energeticness of the access policy and etc. It is necessary to conduct further research to enhance decentralized ABE and hence provide decentralized data access control for un-trusted storage. Operation on Encrypted Data When encryption provides data confidentiality; it also highly limits the flexibility of data operations. To explain this issue, we have to combine ABE with cryptographic primitives such as searchable encryption, private information retrieval and homomorphism encryption to enable computations on encrypted data without decrypting. Moreover, as limitations in terms of data operations supported and efficiency still exist in these cryptographic primitives, another interesting future work would be taking into account information theoretic techniques from the areas such as database privacy. Combining with Secure Computation In this dissertation, we occasionally assumed the servers to be honest-but-curious. In practical systems, it would be beneficial to remove this assumption to provide a stronger level of security protection. In order for doing so, one interesting future work would be integrating techniques from trusted computing into the data access control mechanism.

PROBLEM DEFINITION

We consider a PHR system where numbers of multiple PHR owners and PHR users. The single user having the number of data and number of users who can use the data for his requirement, the owner can update delete and modify the data of his personal files data. it is difficult for the PHR that it maintains numbers of users across the world because the PHR is a internet application, a lot of head ache is there for maintaining the data with that particular owners. Only one central server is there and it is difficult to maintain the username and password of every users and owners. For that we have the solution that we de-centralized the server in disparate locations according to the owners and users requirement where the users are many we use the de-centralized server by which the overhead of the server becomes less in comparison to the previous system. The numbers of users are there and the data must be change or change the policy as per our requirement of the data owner, the management of every data owner and his data and scheme, it is too much overloaded for a single server for that we must divided our server into the distributed style by which the data must be access from anywhere but the load will be minimize from the main server and it is also easy and convenient for the admin and the users and data owners.

REQUIREMENTS

A core requirement is that each patient can control who are authorized to access to her own personal health records documents. Especially, user controlled read/write access and cancellation is the two core security objectives for any electronic PHR system, the security and performance requirements are summarized as follows:

Data Confidentiality: User who wants to access the information without enter the key for that we are making mandatory that everyone should enter the key for data access otherwise user can not access the data by this the data will be secure from the unauthorized users who wants to access the data without the key or by enter wrong secret key.

On Demand Cancellation**:** Whenever a user's attribute is no lengthy valid, the user should not be able to access future PHR files using those attributes. This can be usually called attribute cancellation, and also the corresponding security property is forward secrecy.

Write Access Control**:** In the fields of security and data security, authority control is the precribed restriction of access to a place or other data. The act of accessing may be accessing, modifying, or using. Permission to access a resource is called authorization. By this process we prevent the unauthorized users to hack the data or write the data, that means editing or modifying the data in our storage space, for that we used the ABE algorithm. By the ABE Algorithm we are confident that we are safe from the unauthorized users or hackers.

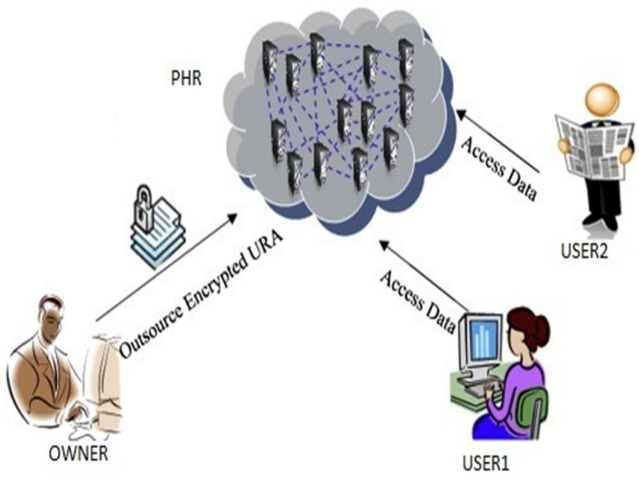

Figure 1: shows scenario of data sharing.

ALGORITHM**:**

1) Encryption: Encryption is the conversion of information from plain text which is understood by people into a form, called a cipher text, which cannot be easily understood by third party people. Decryption is one process of changing encrypted data back into its original state, so it can be understandable.

The use of encryption/decryption is as old as the art of interaction. In wars, a cipher, often incorrectly called as code, which can be hired to maintain the enemy away from obtaining the contents of transfers. (Technically, a logic is a means of representing a signal without the intent of keeping it secret; examples are Morse logic and ASCII.) Simple ciphers contains the substitution of letters for digits, the interchange of letters in the alphabet, and the "scrambling" of voice signals by inverting the bandwidth frequencies. Most complex ciphers work based on sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the content of an encrypted data, the correct decryption key is must be used. The key is an mechanism that rollbacks the work of the encryption mechanism. A computer can be used in an attempt to rollback the cipher. If the encryption algorithm is more complex then it becomes more difficult to eavesdrop on the communications without access to the key.

In our encryption scheme, the message or information is encrypted using a cryptography mechanism called ABE encryption algorithm, turning it into an unreadable cipertext. This is usually done with the use of attribute key, which is also specifies how the message is to be coded. Any third party users that can see the cipher text should not be able to determine anything about the initial data. An authorized party, however, is able to decode the cipher text using a decoded algorithm, that is usually desires a secret decoded key, that the adversaries do not have also access to. For scientific reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.

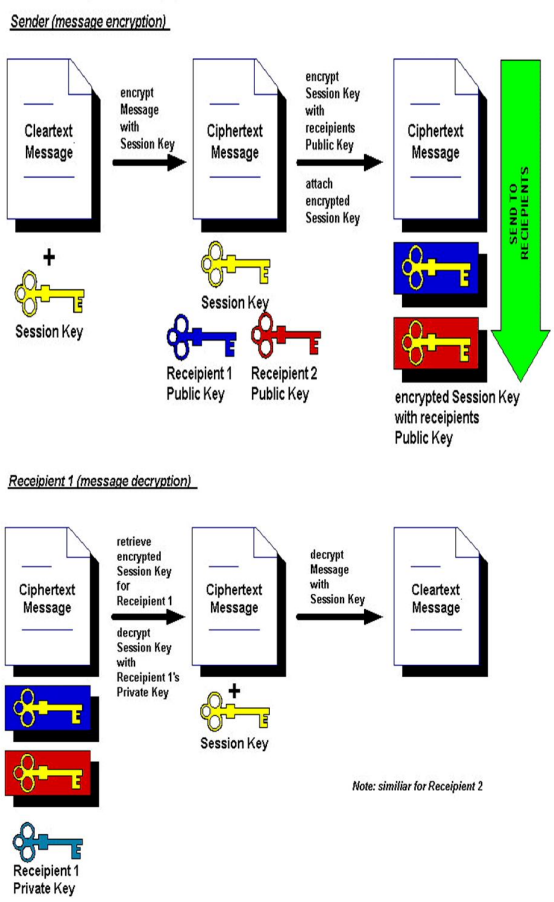

Figure 2: data encryption and key generation

2) Key Generation**:** In key generation we use a attribute based encryption, that means at the time of encryption the keys will generate with the encryption. These keys will be used further for open or decrypt the data.

*3).*Key Update*:* when any user want to access the data, before of that it enters the key for decrypt the data, if the key is valid then he will be able to access the data otherwise if the key is wrong then one notification is send to the owner about that particular users, on the behalf of that user the owner update the key of that particular file.

*4).*Decrypt**:** when the user want the data or file for his/her requirement before of that the data must be decrpt by the use of that key which are given by the user, due to decryption the user will be able to red/understand that particular file.

GAINS:

PHRs grant patients access to a wide range of health data sources, that the best medical experiments and personal health data. All of a user's medical records are stored in one place instead of paper-based files in various doctors' offices. Upon bump into a medical action, a patient's personal health information is only a few clicks away.

Moreover, PHRs can gain clinicians. PHRs offer patients the opportunity to submit their data to their doctor PHRs. This helps doctors give better treatment decisions by providing more continuous data.

PHRs have the potential to help analyze an individual's health profile and identify health threats and improvement opportunities based on an analysis of medicine interaction, current best drug experiments, gaps in current drug care plans, and also identification of drug errors. Patient illnesses can be tracked in conjunction with healthcare providers and early interventions can be promoted upon bump into deviation of personal health status. PHR is also makes it easier for doctors to care for their patients by facilitating continuous contact as disputed to episodic. Eliminating contact barriers and allowing documentation flow between patients and clinicians in a timely fashion can save time consumed by face-to-face meetings and telephone contact. Improved contact can also ease the process for patients and caregivers to quiz the questions, to set up appointments, to request refills and referrals, and to report problems. Plus, it is in the case of an emergency a PHR can quickly provide critical information to proper diagnosis or treatment.

ATTRIBUTE BASED-ENCRYPTION FOR FINE GAINED ACCESS CONTROL OF ENCRYPTED DATA

When we share or store the tricky data from the users by the third party vendors there is a need to encrypt the data before sending the data to the third party vendor or these sites. In previous system one drawback is there is that the encrypted key is given by the third party, by that the data stolen chances is very high by the side of internal employee of third party vendor. Now we propose a new cryptographic way known as re-grained sharing of encrypted data that we call as a key policy attribute based Encryption. In this scheme the key will be generated automatically on the dependency of attribute of plain text, no one can know the key of your data and due to the encryption there is no fear to stole the data from the unauthorized users . In our System the log will be created for every action which are happening in our application.

Let us assume one example by which we explain the encryption scheme, pankaj is a person who wants to upload or share his data to the asif or also from the others users, so when the pankaj upload his data at that moment he encrypt his data and with the encryption the key will be automatically generated and sends to the users as well as data owner, if the panjak do not want to share some data to the users then he passes his request to the third party and the third party do not give the permission to access the data from the database it is normal user or hacker. By that process the data will be the safe. When the asif want to access the data from the third party before of that the key will be included, now it must match with initial key then data will be access otherwise it gives the message upto three time after that that user will be blocked.

CONCLUSION

In our proposed paper, we are mainly concentrated on security of data which are stored or shared with the other users in personally or in publically, for that we are used the cryptographic security system which we can change the plain text into the cheaper text and also use the re-gained access policy which is known as KP-ABE Encryption, the algorithm which we are used in this paper is known as Attribute Based Encryption(ABE), which encrypts the data on the basis of attribute of plain text and generate the key for that particular text, by the use of that particular key the user only access the data what he/she wants but if the user enters the disparate key means not the initial key then up to the three chances it gives the access to try another key, after of three access it will blocks that particular user and sends one intimation mail message to the data owner that the particular user denied to access the data due to his three wrong keys. Since the encryption is used the chances of data stolen and hacking of data becomes too less in comparison of previous system.

REFERENCES

A. Sahai, J. Bethencourt, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In 2007.

G. Bleumer, M. Blaze, and M. Strauss. Divertible Protocols and Atomic Proxy in Cryptography. In *Proc. of EUROCRYPT '98*, Espoo, Finland, 1998.

V. Goyal, Boldyreva, and V. Kumar. Identity-based Encryption with Efficient Cancellation. In *Proc. of* CCS'08, Virginia ,Alexandria, USA, 2008.

D. Boneh and M. Franklin. Identity-Based Encryption from The Weil Pairing. In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.

S. Yu, K. Ren, J. Li. Defending , W. Lou, and Against Key Abuse Attacks in KP-ABE Enabled Program Systems. In *Proc. of Securecomm'09,* Athens, Greece, 2009.

S. Narayan, R. Safavi-Naini, M. Gagn´e, and"Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.

X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in *AHIC 2010,* 2010.

L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption,".

J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE S& P '07,* 2007, pp. 321–334.

A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: security protocols for sensor networks," *Wirel. Netw.*, vol. 8, pp. 521–534, September 2002.

AUTHORS PROFILE

T. Raj Kumar Pursuing M.TECH(CSE) from Holy Mary Institute of Technology and Science, Keesara, Hyderabad Affiliated to JNTU, Hyderabad, Andhra Pradesh, India

Mr. G. Charles Babu, working as an Professor & Head of Computer science Engineering Department in Holy Mary Institute of Technology and Science, Keesara, Hyderabad Affiliated to JNTU Hyderabad, Andhra Pradesh, India.