HIDDEN CIPHER TEXT POLICY ABE WITH PATIENT HEALTH RECORD SYSTEM

BELLAPU BHAVANI [#1], K.RAMBABU [#2]

[#1] MCA Student, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Head & Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

Abstract

In current days almost all small scale and large scale organizations try to adopt the centralized cloud server for their data storage and accessing from the remote locations connected all together from a centralized server with the help of internet. The traditional cipher text-policy attribute-based encryption (CP-ABE) is used to encrypt the data and then send the encrypted data along with keys to the storage server, which will leave a path for attackers to attack the data with that access key. Hence in this proposed application we try to use CP-ABE method on cloud server for encrypting the data and send only encrypted data to the cloud server.Here the keys which are required for encryption will not be send to the centralized server rather than they are send from key-authority which is used for giving keys for the users who request.

Keywords :

Cipher Text, Attribute Based Encryption, Cloud Server

1. INTRODUCTION

The growing industry of cloud has provide a service paradigm of storage/computation outsourcing helps to reduce users' burden of IT infrastructure maintenance, and reduce the cost for both the enterprises and individual users [1], [2], [3]. However, due to the privacy concerns that the cloud service provider is assumed semi-trust (honest-butcurious.), it becomes a critical issue to put sensitive service into the cloud, so encryption or obfuscation are needed before outsoucing sensitive data - such as database system - to cloud [4], [5], [6].

The typical scenario for outsouced database is described in Fig. 1 as that in CryptDB[7]: A cloud client, such as an IT enterprise, wants to outsource its database to the cloud, which contains valuable and sensitive information (e.g. transaction records, account information, disease information), and then access to the database (e.g. SELECT, UPDATE, etc.) [8], [9], [10], [11], [12]. Due to the assumption that cloud provider is honest-but-curious [13], [14], the cloud might try his/her best to obtain private information for his/her own benefits. Even worse, the cloud could forward such sensitive information to the business competitors for profit, which is an unacceptable operating risk.

The privacy challenge of outsouced database is two-hold.

1) Sensitive data is stored in cloud, the corresponding private information may be exposed to cloud servers;

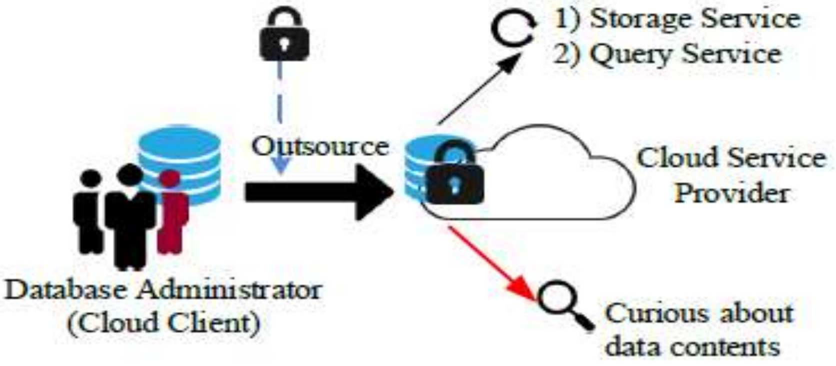


Fig. 1. Outsourced database, service and the privacy risk

2) Besides data privacy, clients' frequent queries will inevitably and gradually reveal some private information on data statistic properties. Thus, data and queries of the outsouced database should be protected against the cloud service provider.

METHODOLOGY

The purpose is to design an secure sharing of personal health records or patient health records in the cloud by encrypting all the PHR dividing the cloud server into two individual partitions for giving access for the data.All the data will be stored in an encrypted manner and those files can be viewed in plain text by the valid users who is allowed by the PHR Owner who uploaded the data and for this they need to substitute the Re-encryption key which is generated by the SRS server.The traditional cipher text-policy attribute-based encryption (CP-ABE) provides the fine-grained access control policy for encrypted PHR data, but the access policy is also sent along with cipher text explicitly. However, the access policy will reveal the users' privacy, because it contains too much sensitive information of the legitimate data users. Hence, it is important to protect users' privacy by hiding access policies. In the proposed system we try to construct a third party department like Authority in order to check all the user tasks and provide access permissions for the end users. By integrating this authority module, we can give guarantee security for the data by taking some public parameters and we can also use constant size for decryption

2. LITERATURE SURVEY

Cloud computing is the utilization of processing assets (equipment and programming) that are conveyed as an administration over a system (normally the Internet). The name originates from the regular utilization of a cloud-formed image as a deliberation for the perplexing foundation it contains in framework outlines. Distributed computing endows remote administrations with a client's information, programming and calculation. Distributed computing comprises of equipment and programming assets made accessible on the Internet as oversaw outsider administrations. These administrations regularly give access to cutting edge programming applications and top of the line systems of server PCs.

RELATED WORK

1) Public Key Encryption with Keyword Search.

Author: D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano.

We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice’s public key. An email gateway wants to test whether the email contains the keyword “urgent” so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word “urgent” is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

2. VABKS: Verifiable Attribute-Based Keyword Search Over Outsourced Encrypted Data.

Author: Q. Zheng, S. Xu, and G. Ateniese.

It is common nowadays for data owners to outsource their data to the cloud. Since the cloud cannot be fully trusted, the outsourced data should be encrypted. This however brings a range of problems, such as: How should a data owner grant search capabilities to the data users? How can the authorized data users search over a data owner's outsourced encrypted data? How can the data users be assured that the cloud faithfully executed the search operations on their behalf? Motivated by these questions, we propose a novel cryptographic solution, called verifiable attribute-based keyword search (VABKS). The solution allows a data user, whose credentials satisfy a data owner's access control policy, to (i) search over the data owner's outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations. We formally define the security requirements of VABKS and describe a construction that satisfies them. Performance evaluation shows that the proposed schemes are practical and deployable.

3. Fuzzy identity-based encryption.

Author: A. Sahai and B. Waters.

We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω 0 , if and only if the identities ω and ω 0 are close to each other as measured by the “set overlap” distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term “attribute-based encryption”. In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

4. Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions.

Author: M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi.

We identify and fill some gaps with regard to consistency (the extent to which false positives are produced) for public-key encryption with keyword search (PEKS). We define computational and statistical relaxations of the existing notion of perfect consistency, show that the scheme of [7] is computationally consistent, and provide a new scheme that is statistically consistent. We also provide a transform of an anonymous IBE scheme to a secure PEKS scheme that, unlike the previous one, guarantees consistency. Finally we suggest three extensions of the basic notions considered here, namely anonymous HIBE, public-key encryption with temporary keyword search, and identity-based encryption with keyword search.

3. EXISTING SYSTEM

In the existing cloud servers ,there was no concept like encryption of cloud data and also there was no facility like key generation and maintenance of data. The current cloud storage is almost centralized and all the data which is stored along with details of data owners and data users is clearly visible by the cloud server department, which is almost a big problem in the current cloud service providers. In some existing clouds there is encryption for the data which is stored inside the cloud and the data along with key details are send for the cloud which is one of the big problem which can leakage the data by un-authorized users who gather that key illegally. Hence the primitive cloud server is not providing full security for the data.

LIMITATION OF EXISTING SYSTEM

1) In the existing or current clouds the following are the main limitations that are available
2) All the existing schemes are limited to the single-owner model.
3) The existing cloud servers are almost operated in a centralized manner, where all the access can be viewed and monitored by the cloud service providers.
4) The existing cloud servers don't have a facility to access the data in a secure manner under dynamic access control.
5) There is no concept like allowing permissions dynamically from the third party controller and in turn has no privilege to restrict the un-authorized users.
6) All the existing methods try to exhaust a lot of time in identifying and provide cure for the infected plant.

4. PROPOSED SYSTEM

The traditional cipher text-policy attribute-based encryption (CP-ABE) provides the fine-grained access control policy for encrypted PHR data, but the access policy is also sent along with cipher text explicitly. However, the access policy will reveal the users' privacy, because it contains too much sensitive information of the legitimate data users. Hence, it is important to protect users' privacy by hiding access policies. In the proposed system we try to construct a third party department like Authority in order to check all the user tasks and provide access permissions for the end users. By integrating this authority module, we can give guarantee security for the data by taking some public parameters and we can also use constant size for decryption

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system:

1. Our protocol supports CP-ABE scheme model with cryptographically parameters to enable more security in real world.
2. At the same time, the privacy of the user is also preserved. The cloud system only knows that the user possesses some required attribute, but not the real identity of the user.
3. To show the practicality of our system, we simulate the prototype of the protocol.
4. The proposed cloud servers have a facility to access the data in a secure manner under dynamic access control.

There is a new concept like allowing permissions dynamically from the Authority module and it can restrict the un-authorized user access

5. SOFTWARE PROJECT MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed protocol. The application is divided mainly into following 4 modules. They are as follows:

1. **Data Owner Module**
2. **Data User Module**
3. **Cloud Module**
4. **Authority Module**

Now let us discuss about each and every module in detail as follows:

5.1 DATA OWNER MODULE

In this module, the provider requests for symmetric encryption key permission from OWNER and upload the patient details in ABE with the key. View & delete the uploaded patient details, and view the clinical report from the user.

5.2 DATA USER MODULE

In this module, user register and logs in and request access control from the healthcare server and view the access control (1-access only the patient details and 2-accessing both patient details with the document), if the user has both the access permissions, user can provide the clinical report for the corresponding patient details.

5.3 CLOUD SERVER MODULE

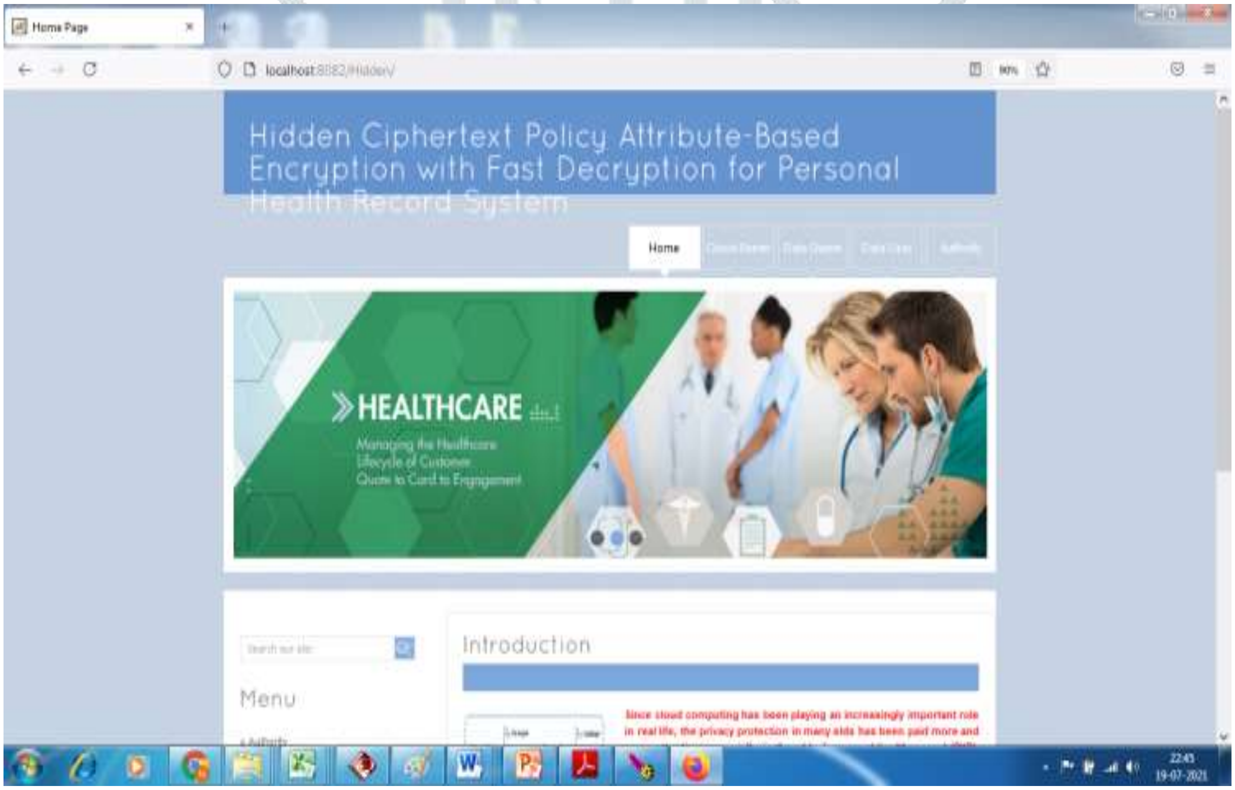
The Cloud Server authorizes both user and owner, view all the uploaded patient details and give the access control permissions to the corresponding requested user. View the response from the OWNER about the key requested. After the clinical report is generated by the user forward it to the corresponding patient. And view the patient disease in chart

5.4 AUTHORITY MODULE

In this module, the Authority will generate the key requested by User. And also generates the symmetric encryption key and provides permission requested by the users.

6 .EXPERIMENTAL RESULTS

1) HOME PAGE



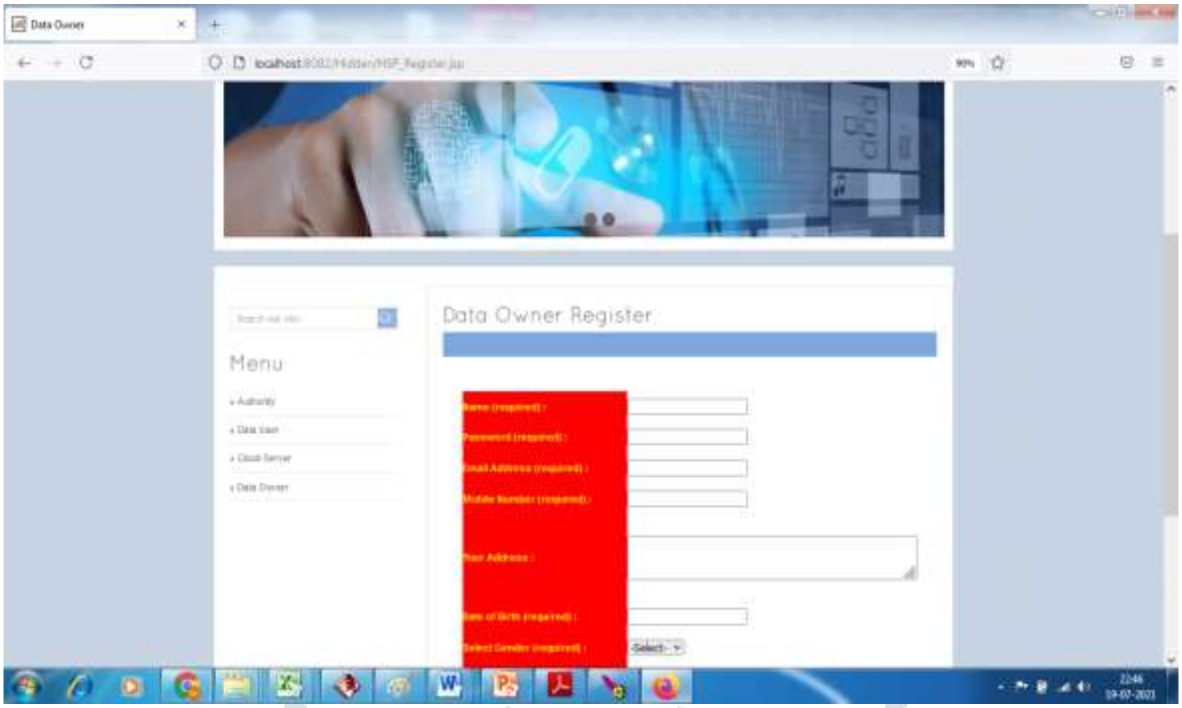
Hidden Ciphertext Policy Attribute-Based Encryption with Fast Decryption for Personal Health Record System

Introduction

Since cloud computing has been playing an increasingly important role in real life, the privacy protection in many fields has been paid more and

Represents the Home Page for the Proposed Application

2) DATA OWNER/DATA USER REGISTRATION NEEDS THE FOLLOWING

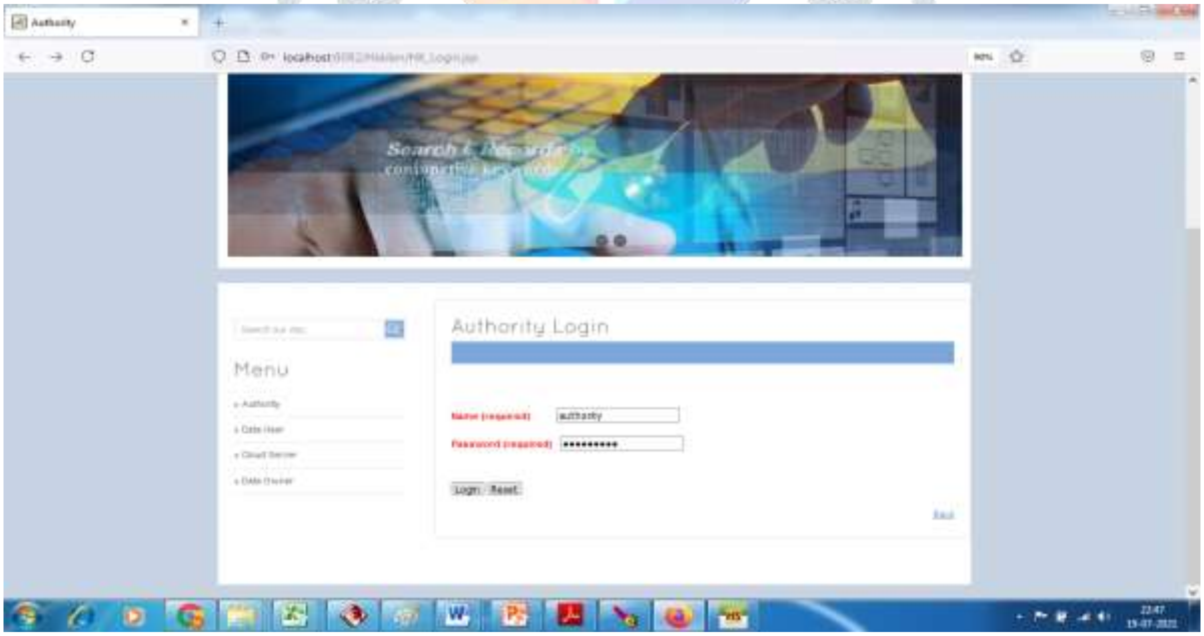


Data Owner Register

Name (required) :
Password (required) :
Email Address (required) :
Mobile Number (required) :
Your Address :
Date of Birth (required) :
Select Gender (required) :

Represents the Data Owner Registration Page for the Proposed Application

AUTHORITY LOGIN

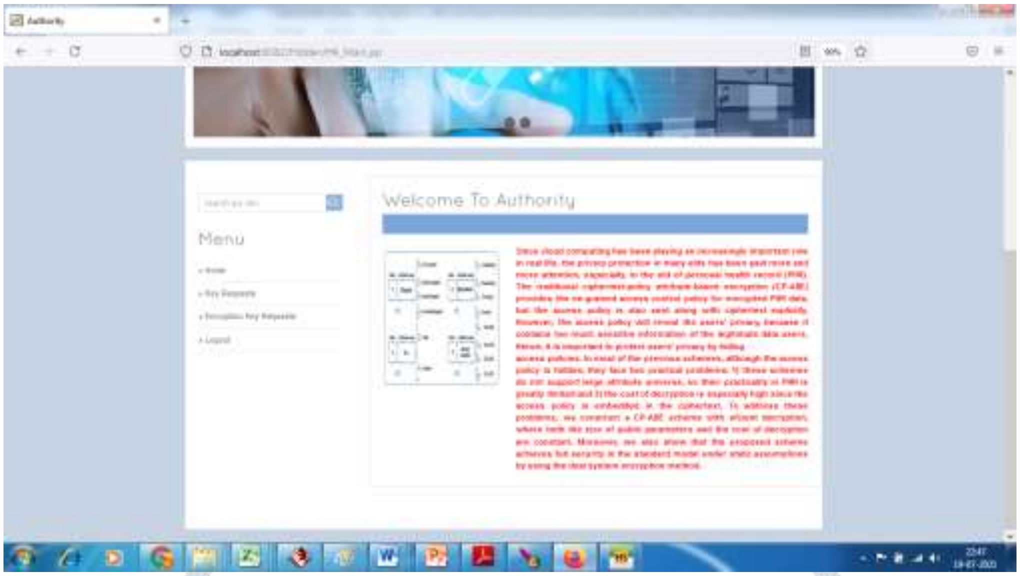


Authority Login

Name (required) authority
Password (required) ••••••••••

Represents the Authority LOGIN

AUTHORITY MAIN PAGE

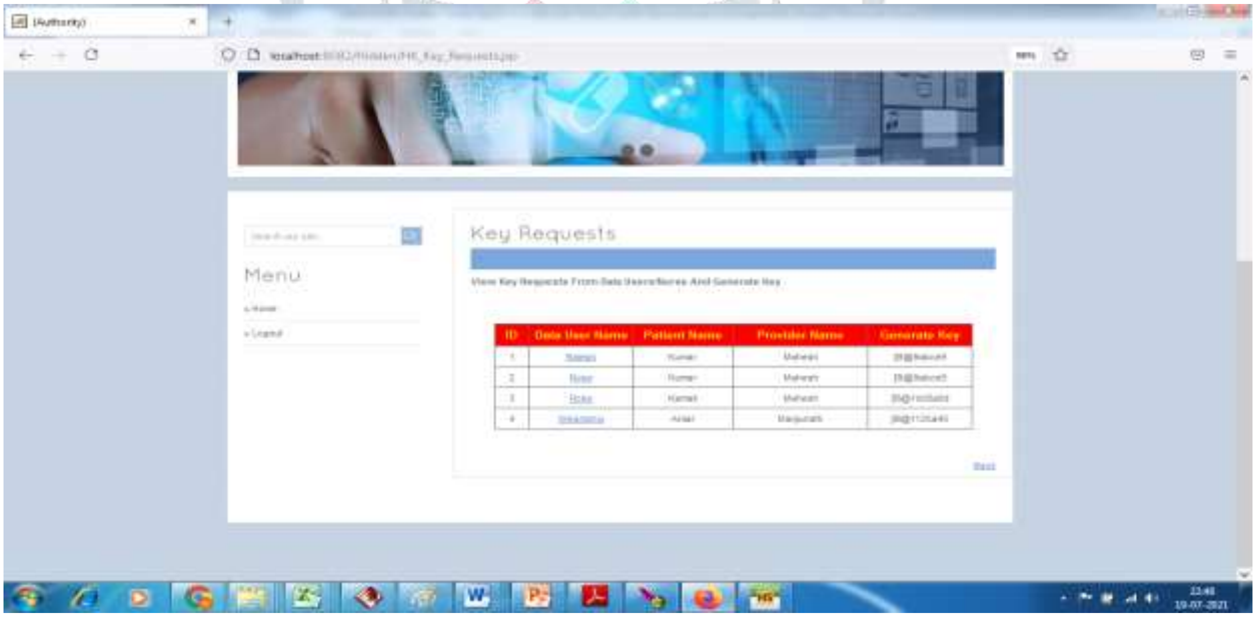


Welcome To Authority

Since cloud computing has been playing an increasingly important role in real life, the privacy protection in many fields has been paid more and more attention, especially, in the field of personal health record (PHR). The traditional ciphertext-policy attribute-based encryption (CP-ABE) provides the fine-grained access control policy for encrypted PHR data, but the access policy is also sent along with ciphertext explicitly. However, the access policy will reveal the users' privacy, because it contains too much sensitive information of the legitimate data users. Hence, it is important to protect users' privacy by hiding access policies. In most of the previous schemes, although the access policy is hidden, they face two practical problems: 1) these schemes do not support large attribute universe, so their practicality in PHR is greatly limited and 2) the cost of decryption is especially high since the access policy is embedded in the ciphertext. To address these problems, we construct a CP-ABE scheme with efficient decryption, where both the size of public parameters and the cost of decryption are constant. Moreover, we also show that the proposed scheme achieves full security in the standard model under static assumptions by using the dual system encryption method.

Represents the Authority HOME PAGE

AUTHORITY VIEWS THE KEY REQUEST



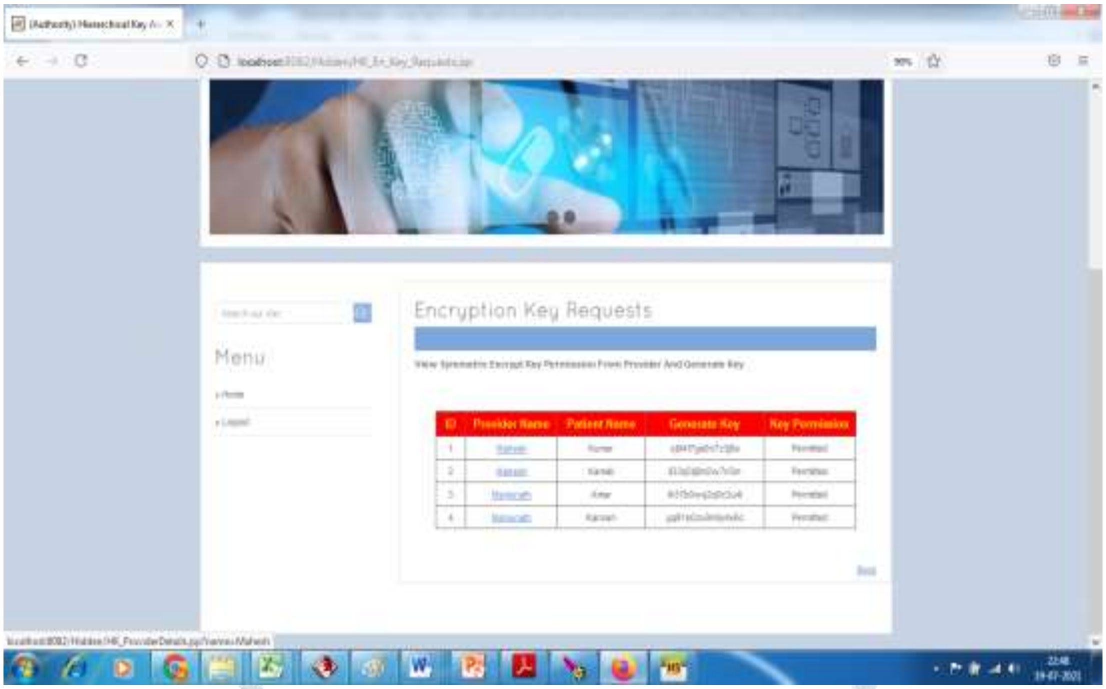
Key Requests

View Key Requests From Data Users/Nurses And Generate Key

ID	Data User Name	Patient Name	Provider Name	Generate Key
1	[illegible]	Kumar	Mahesh	[illegible]
2	[illegible]	Kumar	Mahesh	[illegible]
3	[illegible]	Kamal	Mahesh	[B@[illegible]
4	[illegible]	Ankit	Manjunath	[B@[illegible]

Back

AUTHORITY VIEWS THE ENCRYPTION KEY REQUEST



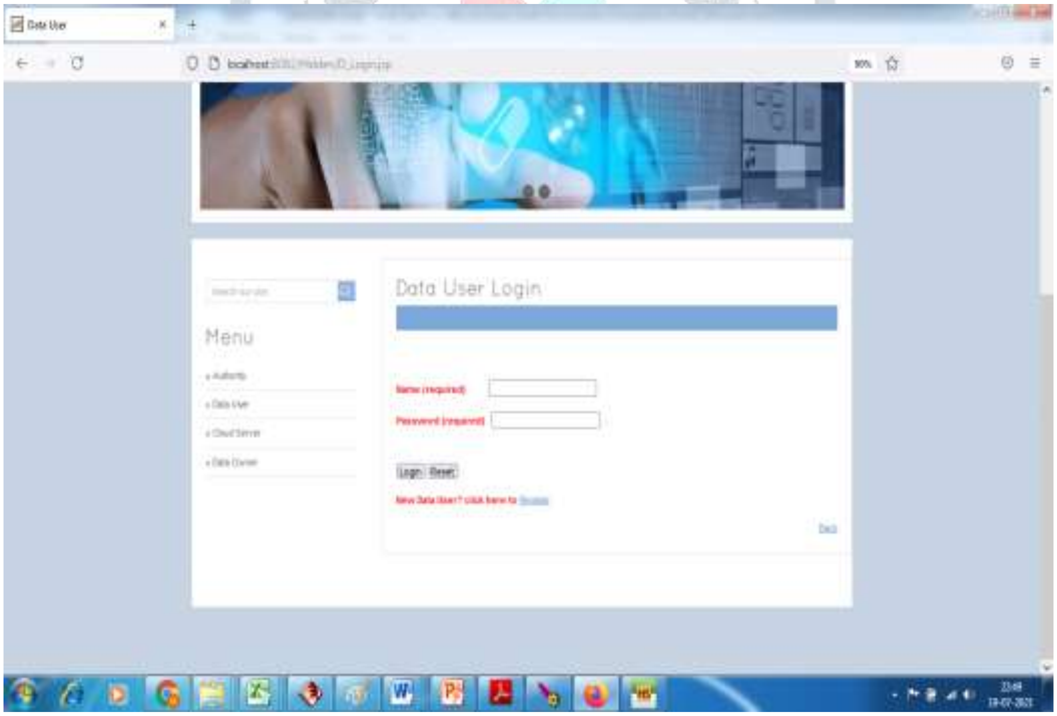
Encryption Key Requests

View Symmetric Encrypt Key Permission From Provider And Generate Key

ID	Provider Name	Patient Name	Generate Key	Key Permission
1	Mahesh	Kumar	[illegible]	Permitted
2	Mahesh	Kamala	[illegible]	Permitted
3	Manjunath	Amar	[illegible]	Permitted
4	Manjunath	Karnan	[illegible]	Permitted

Back

DATA USER LOGIN



Data User Login

Name (required)

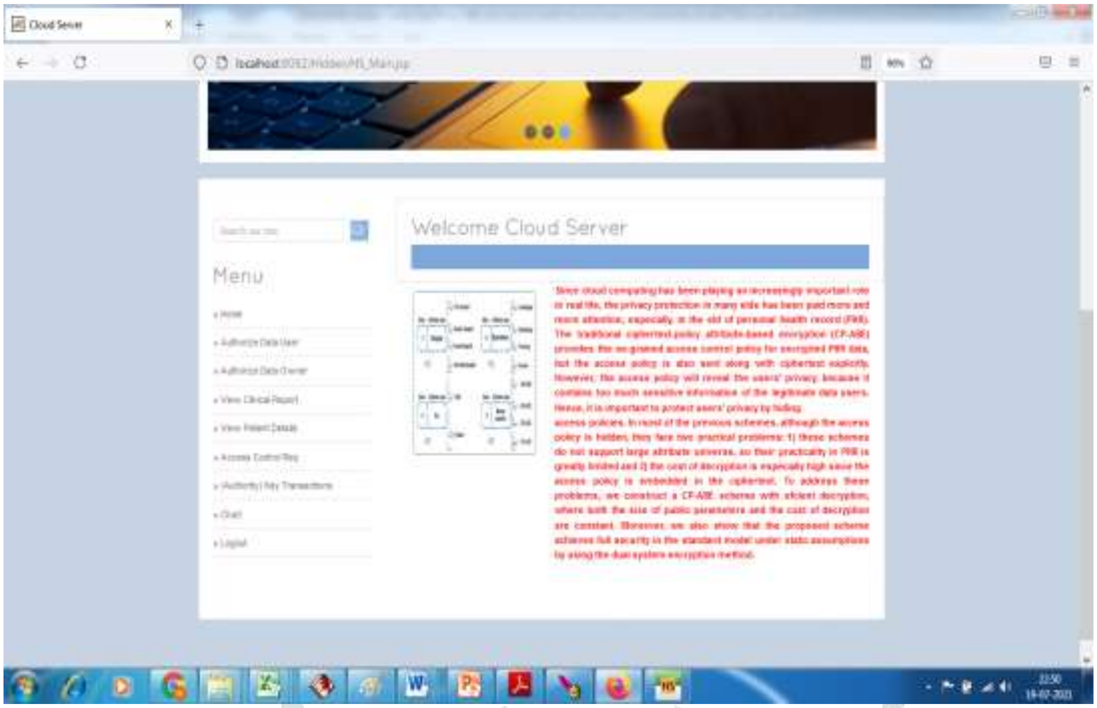
Password (required)

Login Reset

New Data User? Click here to Register

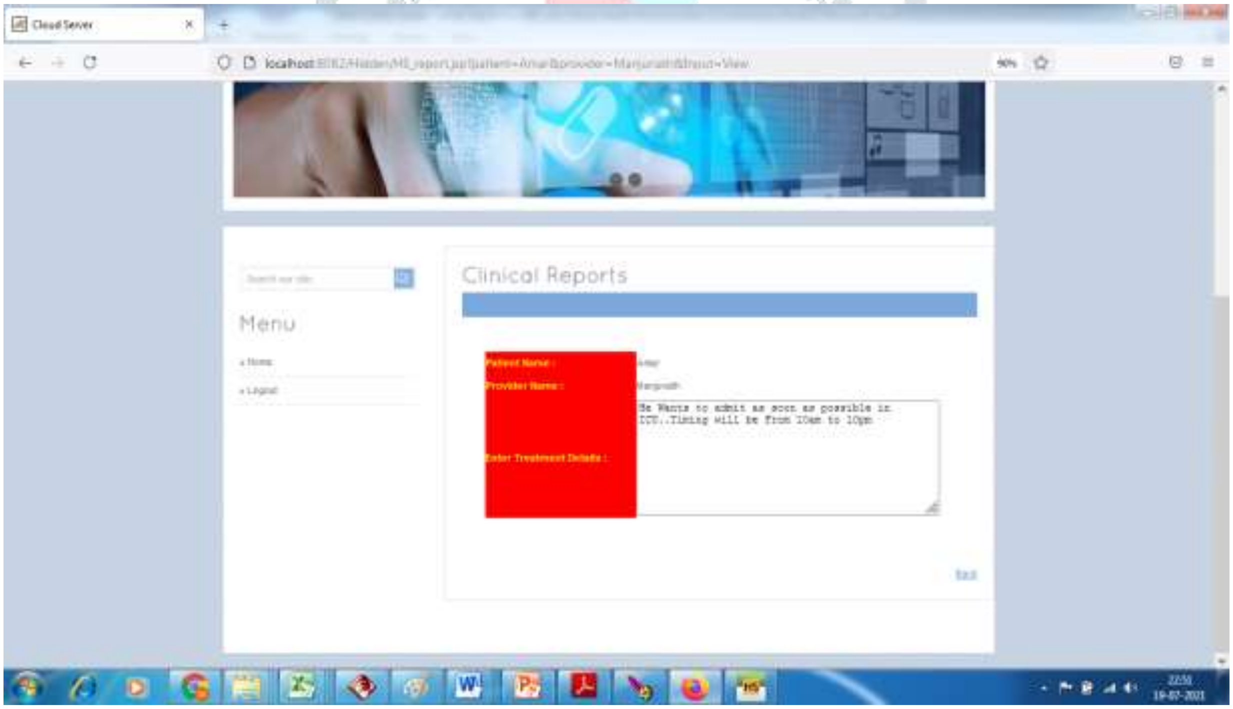
Back

CLOUD SERVER LOGIN



Since cloud computing has been playing an increasingly important role in real life, the privacy protection in many side has been paid more and more attention, especially in the old of personal health record (PHR). The traditional ciphertext-policy attribute-based encryption (CP-ABE) provides the fine-grained access control policy for encrypted PHR data, but the access policy is also sent along with ciphertext explicitly. However, the access policy will reveal the users' privacy because it contains too much sensitive information of the legitimate data users. Hence, it is important to protect users' privacy by hiding access policies. In most of the previous schemes, although the access policy is hidden, they face two practical problems: 1) these schemes do not support large attribute universe, so their practicality in PHR is greatly limited and 2) the cost of decryption is especially high since the access policy is embedded in the ciphertext. To address these problems, we construct a CP-ABE scheme with efficient decryption, where both the size of public parameters and the cost of decryption are constant. Moreover, we also show that the proposed scheme achieves full security in the standard model under static assumptions by using the dual system encryption method.

Cloud Views the Clinical Report of Patient


Cloud Server
localhost:8082/Hidden/MS_report.jsp?patient=Amar&provider=Manjunath&input=View
Clinical Reports
Search our site
Menu
Home
Logout
Back
22:51
19-07-2021

Patient Name : Amar

Provider Name : Manjunath

Enter Treatment Details : He Wants to admit as soon as possible in ICU..Timing will be from 10am to 10pm

7. CONCLUSION

In this proposed work, we introduce a new method called linear secret sharing with multiple values, which can greatly improve the expression of access policy. Moreover, each attribute is divided into two parts, namely the attribute name and its value. Therefore, the most obvious advantage of the proposed scheme is that sensitive attribute values can be hidden. And it can protect users' privacy well in PHR. In the proposed scheme, the size of public parameters is constant and the cost of the decryption is only two pairing operations, which also make it more practical. Eventually, we prove the full security of the proposed scheme in the standard model under static assumptions by using the dual system encryption method. The proposed scheme only achieves partly hiding policy. It is an interesting problem that achieves fully hiding policy with fast encryption, which is left as a future work.

8. REFERENCES

[1] B.Waters, ``Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions,'' in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, Aug. 2009, pp. 619_636.

[2] M. Qutaibah, S. Abdullatif, and C. T. Viet, ``A ciphertext-policy attribute- based encryption scheme with optimized ciphertext size and fast decryp- tion,'' in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, Apr. 2017, pp. 230_240.

[3] B. Waters, ``Ciphertext-policy attribute-based encryption: An expressive, ef_cient, and provably secure realization,'' in *Proc. Int. Workshop Public Key Cryptogr.* Berlin, Germany: Springer, Mar. 2011, pp. 53_70.

[4] V. Goyal, O. Pandey, A. Sahai, and B.Waters, ``Attribute-based encryption for _ne-grained access control of encrypted data,'' in *Proc. 13th ACMConf. Comput, Commun. Secur.*, Nov. 2006, pp. 89_98.

[5] J. Lai, R. H. Deng, and Y. Li, ``Expressive CP-ABE with partially hidden access structures,'' in *Proc. 7th ACM Symp. Inf., Comput. Commun. Secur.*, May. 2012, pp. 18_19.

[6] A. Sahai and B.Waters, *Fuzzy Identity-Based Encryption*, R. Cramer, Eds. Berlin, Germany: Springer, 2005, pp. 457_473.

[7] J. Bethencourt, A. Sahai, and B.Waters, ``Ciphertext-policy attributebased encryption,'' in *Proc. IEEE Symp. Secur. Privacy*, May. 2007, pp. 321_334.

[8] Y. Zhang, D. Zheng, and R. H. Deng, ``Security and privacy in smart health: Ef_cient policy-hiding attribute-based access control,'' *IEEE Inter- net Things J.*, vol. 5, no. 3, pp. 2130_2145, Jun. 2018.

[9] H. Cui, R. H. Deng, G. Wu, and J. Lai, ``An ef_cient and expressive access structures," in *Provable Security_PROVSEC* (Lecture Notes in Computer Science), vol. 10005, L. Chen, Eds. Berlin, Germany: Springer, 2016, pp. 19_38.

[10] C. Y. Umesh, ``Ciphertext-policy attribute-based encryption with hiding access structure," in *Proc. IEEE Inter. Adv. Comput. Conf.*, Jul. 2015, pp. 6_10.

[11] L. Zhang and Y. Hu, ``New constructions of hierarchical attribute-based encryption for _ne-grained access control in cloud computing," *KSII Trans. Int. Information Syst.*, vol. 7, no. 5, pp. 1343_1356, May 2013.

[12] J. Li, K. Ren, B. Zhu, and Z.Wan, ``Privacy-aware attribute-based encryp- tion with user accountability," in *Information Security_PROCEEDINGS* (Lecture Notes in Computer Science) vol. 5735, P. Samarati, Eds. Berlin, Germany: Springer, 2009, pp. 347_362.

[13] J. Li, H. Wang, Y. Zhang, and J. Shen, ``Ciphertext-policy attribute-based encryption with hidden access policy and testing," *KSII Trans. Int. Infor- mation Syst.*, vol. 10, no. 7, pp. 3339_3352, Jul. 2016.
[14] Y. Zhang, X. Chen, J. Li, and D. Wong, ``Anonymous attribute-basedencryption supporting ef_cient decryption test," in *Proc. 8th ACMSIGSAC Symp. Inf., Comput. Commun. Secur.*, May 2013, pp. 511_516.

[15] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, ``A ciphertext- policy attribute-based encryption scheme with constant ciphertext length," in *Information Security Practice and Experience_ISPEC* (Lecture Notes in Computer Science) vol. 5451, F. Bao, H. Li, Eds. Berlin, Germany: Springer, 2009, pp. 13_23.