Password Authentication Scheme Based On Shape and Text for Secure Sharing Of PHR Using ABE in Cloud

Kavitha Murugesan, Anjana.T.K

Abstract*— *Information Technology is widely used in health care for efficiently managing the Personal Health Records (PHR) in a cost effective manner. Under this scenario a computing paradigm (cloud computing) where the resources are provided as services will offer a ubiquitous access to medical data. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. In our paper a hybrid password authentication scheme based on shape and text is used. It uses shapes of strokes on the grid as the origin passwords and allows users to login with text passwords with the help of traditional input devices. Hidden-camera and shoulder-surfing is highly resistible with this approach. The scheme also has high scalability and flexibility to enhance the authentication process security. Such a privacy preserving PHR system should be enforced cryptographically too. We also leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR. Apart from previous works in secure outsourcing of data, multiple data owner scenario is focused, and users in the PHR system is divided into multiple security domains that greatly reduces the key management complexity for owners and users.

IndexTerms*— *Attribute Based Encryption, Cloud Computing, Hybrid Password Authentication, Personal Health Records

I. INTRODUCTION

Health information exchange through PHR has been widely adopted now a days, since they provide a centralized place for owners to create, manage and control their data through web, which makes the storage, retrieval and sharing of data more efficiently. The emergence of Personal Health Records (PHR) has given the patient full control of her data, and can share her data with a wide range of users including health care provider, friends, and family members. The possibilities of digital medical report include minimizing medical errors, save lives, create job opportunities. They also reduce costs in health care by avoiding expensive diagnosis and repetitive drug administration. Building and managing specialized data centers has brought the concept of placing PHRs into third party service providers. Several architectures has been proposed to store PHRs in cloud computing [1][2].

Cloud computing supports storage-as-a-service and software-as-a-service, hence the PHR providers are more willing to shift their storage and application services into the cloud. Personal health data stored in a cloud is always open to potential abuses and threats because the servers cannot provide strong privacy assurance at all. There could be possibilities like if the individual in the cloud provider's organization misbehaves or if the servers are subjected to malicious attack .Potential risks of privacy exposure should be enforced properly. The feasible solution is to defend the unauthorized entry to the PHR system and cryptographically encrypting the data before storing into server. Username and passwords are used as the general method of authentication. Textual passwords are always vulnerable to various attacks as they always contain characters that can be guessed or might be very long for the user himself to remember. Graphical password schemes have been considered as alternatives to traditional text password, but they also have some drawbacks. For example, some of them have vulnerabilities to shoulder-surfing because of the users' direct actions upon the input screen. And some schemes will require users to input the password for more than one time. And also, most of the graphical schemes have far more complexity in the implementation of the application. This work is proposed to make a bridge between the graphic and text password. Since the shape as the password is easier to remember, we take the advantage of the shape as the users' original passwords. To make the implementation easy and avoid direct interaction appeared between the user and screen, a grid with characters is adopted to construct the new system. With this new authentication scheme, users can only just remember the shapes and strokes they like as their passwords. However, the system authenticates the shape passwords just with text on the grid and their input order during the process.

For ensuring more security to the system it would be more effective if the PHR owner herself decide how to encrypt and which set of users are allowed to access each file. Such a "patient centric"PHR system allows access to the users who are given the corresponding decryption key. Scalability and fine-grained access of PHRs is much a challenging issue in a patient centric PHR system. As formerly noted patients can define role-based access right for users. For example they can give full access right to their doctor, but only limited access to their fitness trainer. Such a system is accessible from anywhere due to its centralized management. There are different encryption schemes and they itself define the access structure. For fine grained access and scalability of stored data in untrusted servers like cloud it is better to encrypt data with certain cryptographic primitives and disclosing decryption keys only to authorized users. This type of approach introduces complexity on key management and encryption. To resolve this issue a per-file access control list (ACL) can be adopted. Complexity on ACL depends on the number of users in the system. There can be different types of users; they may need to access the PHR for personal or professional use. Personal users may include family members and

Manuscript received on May, 2013.

Kavitha Murugesan, Department of Computer Science, University of Calicut,Vedavyasa Institute of Technology, Malappuram, India.

Anjana.T.K,Department of Computer science , University of Calicut Vedavyasa Institute of Technology, Malappuram, India.

friends and latter has potentially large scale including pharmacists, fitness trainers, researcher's .Therefore the data owner will be overwhelmed by key management issues in the case of professional users.

In our paper we address this complex key management issues. To solve these issues users are divided into two domains namely public and personal domain. Keys required by professional users are managed by public domain and the users have to manage the keys of a small number of users in her personal domain. This helps to share PHRs among different users as per their needs. This setting is called multi-owner design. In practical application each data file will be associated with a set of attributes. Thus a unique logical expression can be defined for each user based on the attributes to reflect the files that are allowed to access by the user. Fine-grainedness of data access is obtained as the logical expression can represent any desired data file set. Using public key component that are assigned for each attribute data files are encrypted. Secret keys of user are defined to reflect their access structure and so a user can decrypt a cipher text if the data file attributes satisfy his access structure. In the case of public domain multi-authority scheme is established. There exist attribute authorities (AAs) to govern a disjoint subset of user role attributes. In the personal domain owners can directly give access privileges for personal users and can encrypt a PHR under its data attributes.

II. RELATED WORK

This paper is mostly related to works in textual and graphical authentication schemes along with cryptographically enforced access control and attribute based encryption. A graphical password scheme, in which a password is generated through asking the user to click on a graphic or an image provided by the system, is designed by Blonder [3]. When creating a password, the user is asked to choose four images of human faces from a face database as their own password. In the authentication stage, users must click on the approximate areas of those locations. This method is considered as a more convenient password scheme than textual scheme, for the image can help users to recall their own passwords. Wiedenbeck, et al. [4] extended the approach and proposed a system called "Pass Point". It allows users to click on any locations on the image to create the passwords. The system will calculate a tolerance around each pixel which has been chosen. The users must click within the tolerance of the chosen pixels. Jansen [5-7] proposed a graphical password scheme for mobile devices. During enrollment, a user is asked to choose the theme consists of photos in thumbnail size and set a sequence of pictures as a password. In the authentication stage, a user must input the registered images in the correct order. Each thumbnail image is assigned a numerical value, thus the sequence of the chosen ones will create a numerical password. Because the number of picture is limited the password space of this scheme is not large. Jermyn, et al [8] proposed a technique call "Draw a Secret (DAS)". This system allows users to create their own passwords by drawing something on a 2D grid. When a user finishes the drawing, the system stores the coordinates of the grids occupied by the picture. During authentication, users must re-draw the picture which had been created by them. The user will be authenticated if the drawing touches the same gird in the right order. The password space of this scheme is proved to be larger than the full text-based password space. Thorpe and van Oorschot [9] analyzed the memorable password space of the DAS.

Graphical dictionaries were introduced and possibilities of a brute-force attack using dictionaries are studied. They showed that a significant fraction of users will choose mirror symmetric password, since people recall symmetric images better than asymmetric images. Thorpe and van Oorschot [10] also studied the impact of password length and complexity property of the DAS scheme as stroke-count . "Grid Selection" technique is proposed to improve the security. It allows users to select a rectangle region as the drawing grid, in which they may input the password. This method increases the DAS password space. Nali and Thorpe [11] have done further research. To overcome the problem of shoulder-surfing , many techniques were proposed. Zhao and Li [12] proposed a shoulder-surfing resistant scheme "S3PAS" The main idea of the scheme is as follows. During the login stage, they must find their original text passwords in the login image and inside the invisible triangle region a click is made. The system integrates both graphical and textual password scheme and has high level security. Man, et al, [13] proposed another shoulder-surfing defense method. In this scheme, a user chooses many images as the pass-objects. There are variants for pass-objects and an unique code is assigned to them. In the authentication stage, the user must type the unique codes of the pass-objects variants in the scenes provided. Although the scheme shows perfect results in defending hidden camera, the user need to remember code with the pass-object variants. Further research based on this method was conducted in [14]. More graphical password schemes have been summarized in a recent survey paper [15]. For fine-grained access control, the traditional public key encryption (PKE)based schemes [16], [17] either results overhead in key management, or by using different users key encrypting multiple copies of a file . To improve upon the scalability of the above solutions, ABE can be used. In Goyal et.al's seminal paper on ABE [18], data is encrypted under a set of attributes so that multiple users who possess proper keys can decrypt the data. This potentially makes encryption and key management more efficient [19]. A fundamental property of ABE is preventing against user collusion. Although ABE and MAABE increases system scalability under some practical scenarios there are some limitations. In work flow based access control scenarios data access right could be given based on users identities rather than their attributes, but ABE does not handle that properly and under such situations one can depend on ABBE(Attribute Based Broadcasting Encryption) [20]. Also in practice credentials from different organizations must be considered equally effective, but the impressibility of encryptor's access policies are limited by MAABE. in that case distributed ABE schemes [21] will be needed.

III. HYBRID PASSWORD SCHEME

The hybrid password scheme[22] based on shape and text is designed not only for the traditional computers but can be used in the mobile devices. The basic idea of our scheme is to make a map from shape to text with strokes of the shape and a grid with text. The map could be constructed quite simple and straight-forward. This mapping not only guides the user to master this scheme with ease, but makes the whole system easy to implement.

Fig. 1 shows the idea of this work. Users should just think some personal shapes and its strokes as their origin password and enter character in the authentication as the login password. The whole process includes two main steps: the password creation step, and the login step. In the basic scheme, we take a simple example to descript the two stages.

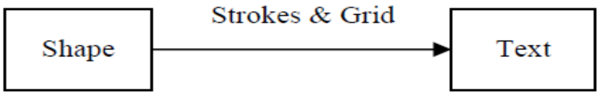
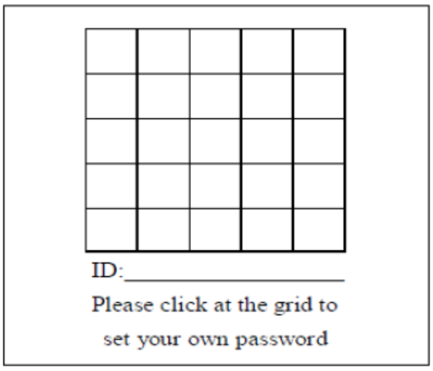


Fig.1: Mapping from shape to text through strokes and grid.

In the first step, the user is asked to select a group of elements on the grid shown in the interface as the original password. In this example, we use g = 5×5 gird to show the process. The password-set interface is shown in Fig.2.



ID:________

Please click at the grid to set your own password

Fig.2: Password Set Interface

Note that the size or the grid (g) can be different to meet the certain requirements and it could affect the security level of the scheme. Firstly, a user is proposed to pick a shape S and it can be a number, a character or even a random shape as his(or her) own original password. The criterion of choosing the shape is as easy to remember as possible for the users themselves. Thus we use one shape to describe this instance for the sake of convenience. After the password shape is selected in their mind, the user should click on the grid in the interface following the shapes' stroke sequence. The system will store the shape and the order with the grid as the user's mapped text password. Suppose the user chooses one of characters of his name "N" as the shape of the password and the sequence of the stroke "N" is in a simpler order than normal as the shape's stroke order. When the shape and the order setting are finished, user could design the stroke on the grid as he likes (this is a mechanism to level up the security level. Even if the shape is known by the hacker in some way, the hacker would not be sure the shape's shape on the grid exactly). After that, the user clicks on the grid to form "N" as the original password. The set procedure can be seen more clearly in the Fig. 3

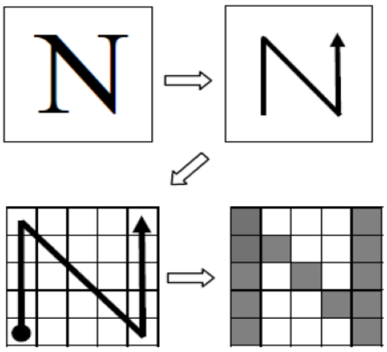
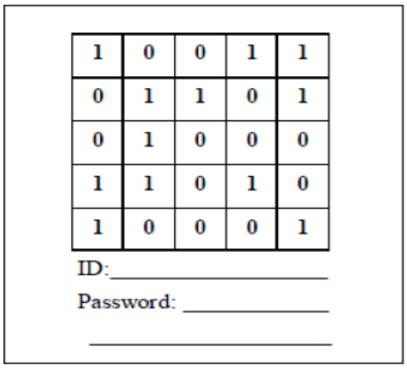


Fig.3: Password Set Procedure

Fig. 3 not only shows the procedure of the setting password, but also provides the idea of mapping from a simple shape into a grid. The shape is finally represented by a number of blocks on the grid. In the login step, the interface is presented with a different style. The grid is filled with some similar symbols such as some numbers or characters. The feature of the approach here is to use quite a few numbers of the symbols, which consists of U. Since the less we use, the faster and more secure of the authentication process will be. Here we use the number "0" and "1" to show the example, which means U = {0, 1}. Note that the system will choose the symbol randomly from U to fill every grid. The login interface is shown in Fig. 4



1	0	0	1	1
0	1	1	0	1
0	1	0	0	0
1	1	0	1	0
1	0	0	0	1

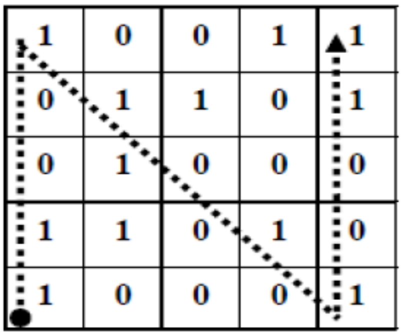
ID:________

Password: ________

____

Fig.4:Login Interface

During the authentication stage, the user was asked to enter the password. He will use the keyboard with only "0"and"1" keys to input the password. The order and content of the password is entering the number in the grid following the original password shape's strokes which he has chosen in the password-set step.



1	0	0	1	1
0	1	1	0	1
0	1	0	0	0
1	1	0	1	0
1	0	0	0	1

Fig.5:Original Stroke on the Interface

While looking at the number filled in the grid of the original shape, user should enter numbers in the right order. Thus, the password is as follows: 1100110110011, where V=[1,1,0,0,1,1,0,1,1,0,0,1,1]. The system will check if the input vector matches the numbers appeared in users original sequence of the grid upon the interface created by the system. Because the texts with which the user enters are only using two keys, the login process is quite convenient. It is very useful to shorten the login process. More importantly, the act of inputting with only two keys can effectively resistant to the shoulder surfing. If the password entered is not correct, then the system will generate another login interface grid for the user with characters randomly selected again. The symbols from U appeared in the grid varies at each login step, which means that the shape and the sequence of shape will not vary but the mapped text will not be the same at different interfaces. It also means the text passwords the user will input are not the same one at different login times. If hackers record the text the user input exclusively, they would get nothing about the information of any user’s original password. Thus the text-based brute force attack with the “1”s and”0”s are resistible. The main idea of the scheme is making the stroke shape as the password using the textual input. And we use this mechanism to resist the spy attack.

IV. PHR SYSTEM MODEL

In this section we describe a patient-centric secure data sharing framework for cloud-based PHR systems.

A. Entities

There are multiple PHR owners and PHR users in a PHR system. Owners can create, delete and manage the data. There exist a central server that stores all the owners PHR.The users come from various domains and to deal with them multi-authority system has been designed into case of public domain.PHR system uses standard data format based on XML data structure.XML helps to organize data in a hierarchical way[16]

B. Framework

Our framework is designed to provide secure patient-centric PHR access and for efficient key management. The key idea is to divide the system into multiple security domains (namely, public domains (PUDs) and personal domains (PSDs)) according to the requirement of the user. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researcher. For each PSD, its users are personally associated with a data owner , and they make accesses to PHRs based on access rights assigned by the owners.

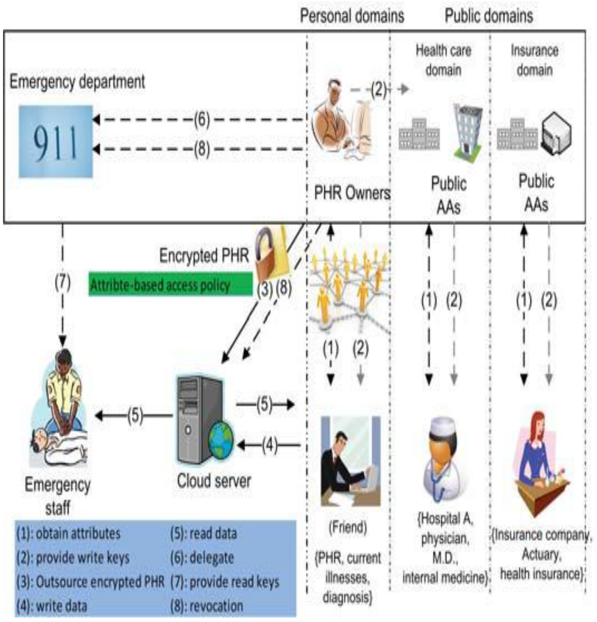


Fig.6.Proposedframework for patient-centric,multi-owner, multi-authority PHR system on cloud

Attribute Authorities(AAs) that deal with PUDs are build up with Role attributes representing the professional role or obligations of a PUD user. Attribute-based secret keys from the AAs, is obtained by user's in PUDs without directly interacting with the owners. Owners are free to specify role based fine grained access policies for her PHR files to control access from PUD users while do not need to know the list of authorized users when doing encryption. PUDs contain the majority of users, and so it greatly reduces the key management overhead for both the owners and users.

V. ATTRIBUTE BASED ENCRYPTION

As more sensitive PHRs are shared and stored in cloud there is always need to encrypt the outsourced data. For fine-grained sharing of encrypted data al Key-Policy Attribute-Based Encryption (KP-ABE) has been developed. In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. If a user want to grant access to a party for all entries on a particular range of dates that have an ID from a particular hospital, the user either needs to act as an intermediary and decrypt all entries for the party or must give the party its private decryption key by letting them access to all entries. Neither one of these options is particularly appealing.

To solve the above problem ABE was introduced. In an ABE system, a user's keys and cipher texts are labeled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key. With a set of descriptive attributes Cipher text will be labeled by the encryptor. Each private key is associated with an access structure that specifies which type of cipher texts the key can decrypt. Such a scheme a is called Key-Policy Attribute-Based Encryption (KP-ABE), since the private key specifies the access structure , while the cipher texts are simply labeled with a set of descriptive attributes. For example, one can specify a tree access structure where the interior nodes consist of AND and OR gates and different parties are presented as leaves. Any set of parties that satisfy the tree can reconstruct the secret.

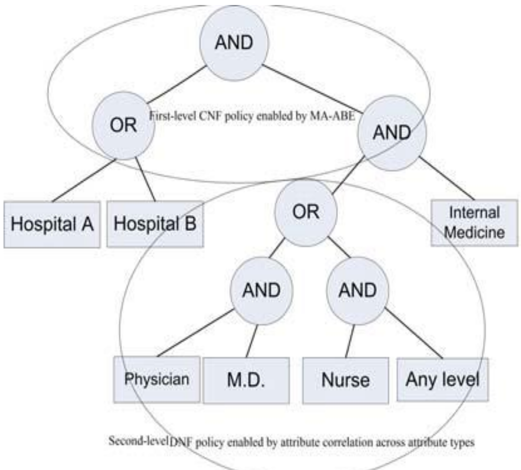

AND
OR
First-level CNF policy enabled by MA-ABE
AND
Hospital A
Hospital B
OR
Internal Medicine
AND
AND
Physician
M.D.
Nurse
Any level
Second-level DNF policy enabled by attribute correlation across attribute types

Fig.7.An example policy realizable under our framework

For instance, if Alice has the key associated with the access structure “X AND Y", and Bob has the key associated with the access structure “Y AND Z", we would not want them to be able to decrypt a cipher text whose only attribute is Y by colluding.. We will show that this cryptosystem gives us a powerful tool for encryption with fine-grained access control for applications such as sharing audit log information. The data that is stored on the server in an encrypted form while different users are still allowed to decrypt different pieces of data per the security policy has been achieved. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access. One can specify a tree-access structure where the interior nodes consist of AND and OR gates and different parties are presented as leaves. Any set of parties that satisfy the tree can come together and reconstruct the secret.

An (Key-Policy) Attribute Based Encryption scheme consists of four algorithms.

Setup This is a randomized algorithm that takes no input other than the implicit security parameter. The public parameters PK and a master key MK are the outputs.

Encryption This is a randomized algorithm that takes as input a message m, a set of attributes Ɣ, and the public parameters PK. It outputs the cipher text E.

Key Generation This is a randomized algorithm that takes as input - an access structure A, the master key MK and the public parameters PK. A decryption key D is the output.

Decryption This algorithm takes as input - the cipher text E that was encrypted under the set Ɣ of attributes the decryption key for access control structure A and the public parameters PK. It outputs the message M if Ɣ belongs to A.

VI. CONCLUSION

In this paper, a hybrid password scheme based on shape and text is proposed. The scheme has salient features as a secure system for authentication immune to shoulder-surfing, hidden camera and brute force attacks. It also has variants to strengthen the security level through changing the login interface of the system. In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. Furthermore, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we show that our solution is both scalable and efficient.

REFERENCES

[1] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, “Securing the e-health cloud,” in *Proceedings of the 1st ACM International Health Informatics Symposium*, ser. IHI ’10, 2010, pp. 220–229.

[2] M. Li, S. Yu, N. Cao, and W. Lou, “Authorized private keyword search over encrypted personal health records in cloud computing,” in *ICDCS ’11*, Jun. 2011.

[3] G. E. Blonder, "Graphical passwords," in United States Patent, vol. 5559961, 1996.

[4] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N.Memon, "Authentication using graphical passwords: Basicresults," in *Human-Computer Interaction International(HCII2005)*. Las Vegas, NV, 2005.

[5] W. Jansen, "Authenticating Mobile Device User Through Image Selection," in *Data Security*, 2004.

[6] W. Jansen, "Authenticating Users on Handheld Devices,"in *Proceedings of Canadian Information Technology Security Symposium*, 2003.

[7] W. Jansen, S. Gavrila, and V. Korolev, "A Visual Login Technique for Mobile Devices," in *National Institute of Standards and Technology Interagency Report NISTIR 7030*, 2003.

[8] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D.Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999

[9] J.Thorpe and P. C. v. Oorschot, "Graphical dictionaries and the memorable space of graphical passwords," in *Proceedings of the 13th USENIX security Symposium,* San Deigo,CA, 2004.

[10] J.Thorpe and P. C. v. Oorschot, "Towards secure design choices for implementing graphical passwords," in *Proceedings of the 20the Annual Computer Security Applications Conference*. Tucson, Arizona,2004.

[11] D. Nali and J. Thorpe, "Analyzing user choice in graphical passwords.," in *Technical Report School of Information Technology and Engineering*, University of Ottawa, Canada, 2004.

[12] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07)*, vol. 2. Canada, 2007, pp. 467-472.

[13] S.Man, D. Hong, and M.Mathews, "A shouldersurfing resistant graphical password scheme," in *Proceedings of International conference on security and management. Las Vergas,* NV, 2003.

[14] D. Hong, S. Man, and B. Hawes, "A password scheme strongly resistant to spyware," in *Proceedings of International conference on security and management*. Las Vergas, NV, 2002.

[15] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," *21st Annual Computer Security Applications Conference (ASCSAC 2005)*. Tucson, 2005.

[16] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient controlled encryption: ensuring privacy of electronic medical records,” in *CCSW ’09*, 2009, pp. 103–114.

[17] C. Dong, G. Russello, and N. Dulay, “Shared and searchable encrypted data for untrusted servers,” in *Journal of Computer Security*, 2010.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in *CCS ’06*, 2006, pp. 89–98.

[19] M. Li, W. Lou, and K. Ren, “Data security and privacy in wireless body area networks,” *IEEEWireless Communications Magazine*, Feb. 2010.

[20] N. Attrapadung and H. Imai, “Conjunctive broadcast and attribute-based encryption,” *Pairing-Based Cryptography–Pairing 2009*, pp. 248–265, 2009.

[21] S. M¨ uller, S. Katzenbeisser, and C. Eckert, “Distributed attributebased encryption,” *Information Security and Cryptology–ICISC 2008*, pp. 20–36, 2009

[22] “Enhanced Authentication Schemes for Intrusion Prevention using Native Language Passwords”,Sreelatha Malempati , Shashi Mogalla

[23] Ming Li, Shucheng Yu and Kui Ren, and Wenjing Lou, Department of ECE, Worcester Polytechnic Institute, USA, Department of ECE, Illinois Institute of Technology, USA, “Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings”