User-centered Security for Protecting Patient Privacy for E-health Cloud Computing*

Mardin A. Anwer
Salahaddin University,
College of Engineering, Iraq
mardinsherwany77@gmail.com

Ingo Stengel
Plymouth University, College of Science and Mathematics
Plymouth, UK
Ingo.Stengel@hs-karlsruhe.de

Rina Dinkha Zarro
Salahaddin University, College of Engineering,Iraq
rina.zarro@yahoo.com

Abstract **E-health is the present communication structure in medicine especially in developed countries. Toward enhancing the quality of care and reduce the health care delivery cost, cloud Computing technology has been adopted. In recent times services such as exchange and share medical data among staff and then to the patients are one the main reasons behind using this technology in e-health. Hence, using cloud computing in e-health has many challenges particularly when dealing with electronic healthcare records (EHR).**

Cloud computing is an agglomeration of technologies, operating systems, storage, networking, virtualisation, each fraught with inherent security issues. For example, browser-based attacks, denial of service attacks and network intrusion become carry-over risks into cloud computing. It differs from traditional computing paradigms as it is scalable which can be encapsulated as an abstract entity to provide different levels of services to the clients.

In this paper, we identified the users of e-health such as doctors, nurses and family members and then their security requirements are identified. An application with five stages toward encryption and decryption process is designed. Since trust is a critical factor in cloud computing, this project will investigate the obstacles that cause this technology lose its credibility in certain clouds. To enhance user authentication process, two-tier mechanisms are used to identify the user's identity. While in confidentiality, it should be assured that information is shared only among authorised people or vendors by applying powerful cryptographic concepts. In this prototype application, the user will be able to protect his/her data and is responsible for providing a high level of security as long as these data are highly private and important.

Keywords- E-Health, Electronic health record , privacy, User-centred Security, User Security Requirements, Multi-tier Authentication, Five Stages Proposed Application.

I. INTRODUCTION

Cloud computing is a modern information technology. Today, many internationally famous companies provide this type of technology to their users such as Google, IBM and Microsoft. Although using this new technology has become very popular, there are many big challenges it faces like security, legal and compliance and organisational challenges.

Recently, there is a growing need for distributing data and information between healthcare teams using cloud e-health. The main advantage of this method is the ability of delivering information easily between the team and making medical decision quickly[1]. What is more using this technology saves time and cost [2]. Hence, the main concern with sharing health information is the privacy; security risks associated with it and trust [1].

The factor of 'trust' is very important; if there seems to be an obvious lack of trust between the healthcare team and Cloud, this technology will be in trouble, and in return, it will never develop. There is a critical need to securely store, manage, share and analyse data in the Cloud. Because Cloud encompasses many technologies, security issue should be a concern.

It is not enough for healthcare members to depend solely on the security given by the companies in the form of "log on account" process. For that reason, a new model with a two-tier authentication process will be introduced in this paper.

After identifying the available security issues and user's fears, a new prototype model was designed. This model is the desktop software that will be installed in the healthcare team and the patient's personal device.

Before designing the model, we started by analysing the user's requirements from the user's perspective in the form of user cases and scenarios.

*This paper was presented at the Third International Scientific Conference of University of Human Development (April, 2016)

These requirements were the goals of the proposed model.

Problem Definition

Security has always been the main issue while adopting Cloud Computing. Since 2008, most surveys and research reports have pointed to the security as the main barrier for not accepting cloud in Information Technology.

The IDC survey conducted in August 2008 has shown that security is the most serious concern for the enterprises ascribed to Cloud Computing. In 2009, security represented 87.5% of overall cloud issues [4], while availability and performance respectively were 83.3% and 82.9%.

A survey conducted by Saugatuck Technology in July 2012 states that data security and privacy as well as data integration concerns are top issues in deploying cloud-based business solutions.

This shows that there are still doubts about the security which discourages the enterprises to adopt Cloud Computing.

Another survey by Ponemon was fielded in 2010 which revealed that fifty percent of organisations are not using Cloud Computing. Ponemon further adds that this situation has remained unchanged since 2010 [5]. The percentage of organisations that considered cloud as more secure than on-promise was 29% in 2010 and it became only 35% in 2012. This means that the use of Cloud Computing is still limited in IT (Information Technology) and it is all because of the security concern that this technology is not making a notable progress. In e-health the data are more vulnerable to attacks compared to other sectors. In fact, the privacy is the key for data in healthcare and any breach in the confidentiality of personal captured data would seriously repulse patients from adopting e-health solutions [3].

II. RELATED RESEARCH

In this section, we will focus on the related work of adopting user center security in cloud computing in general and not just in e-health. Since 2001, protecting customer information is taken as higher priority in the guidelines. Using username and password as the only authentication process in any applications means that the application is under threat.

[7] and [8] state that using two tier authentication or two factor authentication (2FA) mechanisms should be adopted as one tier login password is not enough. That is why users are asked to enter secret code which is sent to their mobile phone.

At present, authentication is done in several ways: such as, textual, graphical, biometric, 3D password and third party authentication. This section will focus on the related research which used two- ties authentication in their proposed design to protected user's data. Also the research that explain how cryptographic concepts can provide security needed for user's data.

Agrawal at el in 2011 [9] proposes a multilevel authentication technique which generates / authenticates the password in multiple levels to access the cloud services. The first level ensures accessing the cloud from cloud vendor so if unauthenticated organization or hackers try to access the cloud services; they are going to terminate in this level itself. Second level of authentication is a team level password authentication/ generation. It is to authenticate the team for particular cloud service. Like this, authentication system can have third, fourth, fifth etc level. Finally, the last level will be the user level password authentication/generation, which ensures that customer/end user has particular privileges and permission.

Another multi-tier authentication scheme in Cloud has been designed and implemented by Singh et al. in 2012 [10]. The first tier authentication uses the encryption/decryption mechanism as followed in normal authentication schemes. While the second requires the user to perform a sequence of programmed activities on the fake screen. This fake screen is loaded by the Cloud server in order to capture second tier authentication details from the user. The sequence of activities which the user performs on the fake screen must be same which he has chosen during registration. If the details entered by the user are correct then the original screen of application is loaded, otherwise, the user is left over the fake screen. Hash function has been used to encrypt the data before sending it to the cloud.

In 2008 [11] proposed a new architecture called PIPE (Pseudonymization of Information for Privacy in e-Health) that integrates primary and secondary usage of health data. they offers an innovative concept for data sharing, authorization and data recovery that allows to restore the access to the health care records if the patients' security token is lost or stolen. [1] in 2013 attempt to spot the issues of privacy and security in the domain of mobile telecare and Cloud computing. The Telecare application allows healthcare to remotely monitor patients via the Cloud in a secure and confidential manner. The key features of their model was the ability to handle large data sizes and efficient user revocation.

In the other hand [3] in 2015 proposed a secure end-to-end protocol to transmit captured data while ensuring confidentiality and authentication. To succeed this goal, they proposed offloading highly consuming cryptographic primitives to third parties. Their results show that the protocol provides a considerable gain in energy while its security properties are ensured.

In 2014 [12] suggest a promising solution for fine-grained access control and secure sharing of signcrypted (sign-thenencrypt). They suggested new primitive Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) which satisfies the requirements of cloud computing scenarios for PHR. CP-ABSC combines the merits of digital signature and encryption to provide confidentiality, authenticity, unforgeability, anonymity and collusion resistance. They have proven the correctness, security and efficiency of this scheme.

Analysis of the Scenarios

For the proposed application, two scenarios are considered:

Scenario One: If we consider that Alice is working as a doctor in one of NHS health centres, she is supposed to keep many of her patients' records in her own device at the NHS centre building. Alice travels because of the courses that she might take to improve her career or to visit other NHS centres that need her help from time to time. Bob is her friend and assistant at the same time. Bob should update Alice with appointments of new patients while she is away and observe the changes that Alice has done in a specific record at the time of updating. Therefore, Alice has decided to use cloud computing as a good idea to have access to the patients' records even when she is at home. The idea of the cloud computing also enables Alice to share some records with Bob and help him know about the changes that she might do.

As a doctor, Alice deals with very sensitive data. These data should remain unchanged, not faked or accessed by other NHS employees except for Bob. Acquaintance with the security issues discussed in the previous chapters that arise while using cloud computing may make her be hesitant about using this technology.

According to this scenario and Alice's requirements which are patients’ records’ integrity, confidentiality, authority (only she who has full access to the record) and the sharing of some records’ links with Bob, we design our first application which meets Alice’s needs and allows her to use it without fear.

Scenario Two: In this scenario, we suppose that Alice does not want to share data with Bob. Instead, she wants him to develop the ability to encrypt the files that contain patients' records before uploading them to the Cloud as well as decrypting files that Alice has encrypted. Accordingly, second prototype has been skilfully designed to meet Alice's requirements.

Specific Cloud Security Requirements/Criteria

Before designing the model, we started by analysing the user's requirements from the user's perspective in the form of user cases and scenarios. These requirements were the goals of the proposed model.The most worrying fact about using and storing data in the cloud is that cloud providers control user's data and as a result can access it. Thus, the first stage considered in designing the model was to transfer the control over to the user.

The second significant stage was adopting a powerful encryption algorithm for encrypting the data. This requires the attackers to have expensive resources and exert much effort to reach the original content. Through this mechanism, the user’s privacy will be protected from any risks from within the Cloud. The overall benefit of this process is that the cloud service provider has no knowledge at all of the user's data.

Like many other software, confidentiality was an essential requirement. Besides, the form of protecting data integrity (protection from modification) and confirmation of the identity of the sender (authentication) were the other two requirements.

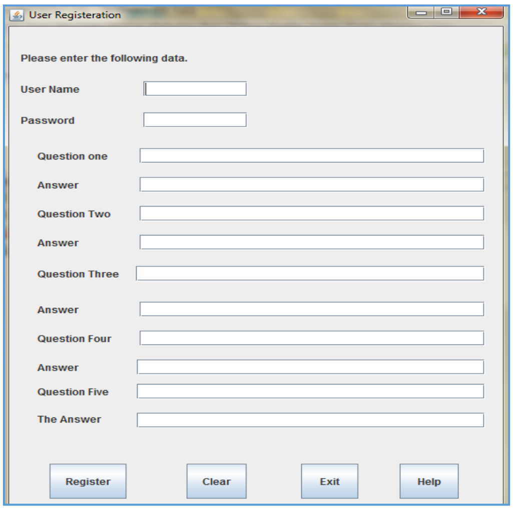
Because the secrecy is not in the algorithm, but in the key (Kerckhoffs's principles 1883) (Kahn, 1973), therefore the last requirement had to be key management. If the key generates, encrypts, stores and distributes in a professional way, then any attempt by the attackers to access the keys and the system will be circumscribed.The software design stage combines the requirements of the programmer who will write the software and the user who will use it. As a programmer, selecting a language to implement the model has been the key requirement especially with the variety of computer programming languages that are available nowadays. Thus, the selection of a proper language is dependent on different criteria such as the language facilities, pre-defined encryption functions and its library. All this will be done to ensure that the design provides the target security.

However, as a user, there are requirements that the application should meet such as user-friendly interface, simple instructions to follow, explanation of how the program works and the software installs.

III. DEVELOPING AN APPROACH FOR END-USER CENTRED SECURITY IN A CLOUD

To give an overview of the proposed software design, every stage will be explained.

The Registration Stage :This process runs once after installing the application in the user's PC. It requires the user to enter specific information like username, password and five questions with their answers. This information will be used later to verify the user in the first-tier and second-tier authentication stages. There are no restrictions for the length of the data entered. When the user submits the information, the system will create digest messages digests for both the username and password by using the hash function, as the questions and answers will become encrypted and then stored in a text file called cloud file.txt. Figure 1 shows the registration stage.



Please enter the following data.

Figure (1) 'Registration' in the Proposed Application

which were entered earlier in the registration process. The digest messages of the entered data will be created and compared with the saved digest messages in the cloudfile.txt. If the information matches, the user will be able to move on to the second-tier authentication stage.

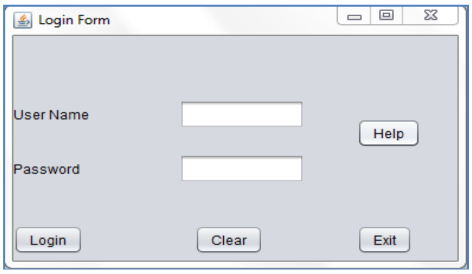
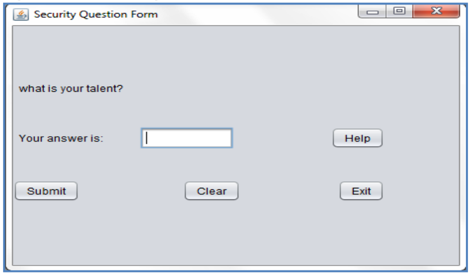


Figure (2) 'Login Form' in the Proposed Application

Second-tier Authentication stage: If the user passes the first-tier authentication process, then they must answer the question that will appear in the form. The system is designed to select the question randomly and it is one of the questions that the user has entered in the registration stage.



what is your talent?

Figure (3) 'Security Question Form' in the Proposed Application

Passphrase and the Generation of Key Stage: In this stage, the user enters their passphrase that will be used to generate the secret key. This key will be used to decrypt the cipher text. The passphrase should be short and easy to remember, as it is not necessary to save it in the system (Ferguson and Schneier, 2003).

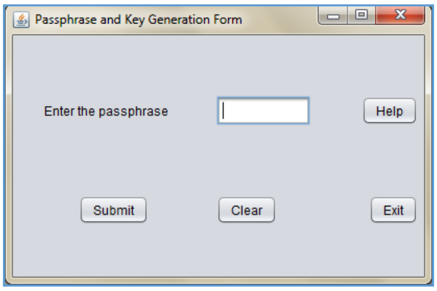


Figure (4) 'Passphrase and Key generation Form' in the Proposed Application

Encryption and Decryption stage :This stage consists of three sub-stages. These sub-stages are file selection, encryption and decryption. In the file selection sub-stage, the user should select a file from his PC or any attached device or cloud storage provider. Then, the user chooses either the encryption or decryption sub-stage.

For the encryption sub-stage, two models were designed. Model one meets the requirements of scenario one while model two meets the requirements of scenario two.

First Encryption Stage Design Model : This model needs six steps to encrypt the selected file before sending it to the Cloud. These steps are a, b, c, d, e, f, g and h which meet the requirements of scenario one.

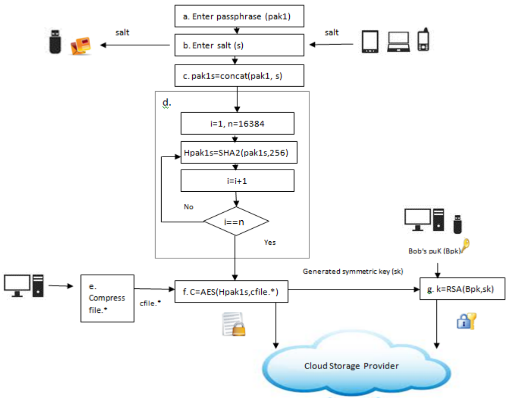


Figure (5) Encryption and Decryption process

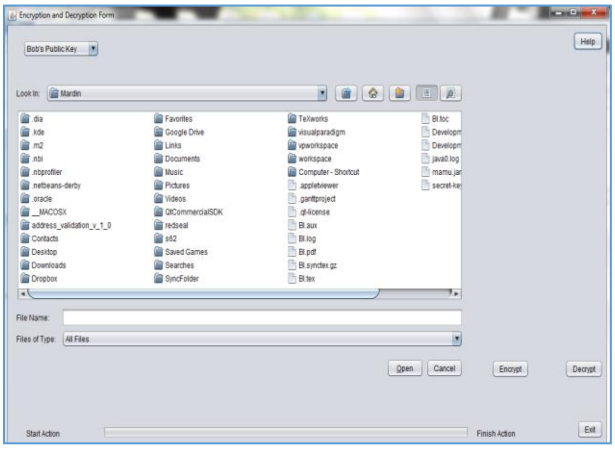
In step (a), Alice must enter her passphrase which is represented by the variable pak1. Alice must keep it secret and should not send it out to other parties. Then, in (b), the salt value must be entered either directly from the attached device or from a file that stores the salt value. Salt is a unique serial number of a specific device, for instance, a smart phone or personal computer (Nanda and Feuerstein, 2005). Step

(c) concatenates the salt and the passphrase that were entered in step (a) to generate the variable (pak1s).

The variable (pak1s) will be hashed 16,384 times in step (d). This operation makes cracking process much more difficult, and is known as key stretching. Hpak1s should be saved in a very safe place because it is Alice's private key which she will use to decrypt the files that Bob sends her.

The selected file needs to be compressed before encrypting. This will be implemented in step (e). Compressing the text increases the security of the message because it places further demands on the cryptanalyst. This compression deprives him or her of the repetitions offered by the user of the alphabetic text. Another advantage of compressing the message is that it will take less modem time when it actually transmits (Hobbit, 2007).

Next is step (f) where the compressed file encrypts using the calculated key with symmetric algorithm AES. To keep the generated symmetric key secure, it will be encrypted using Bob's public key and RSA asymmetric algorithm. Whereas the private key uses to decrypt the key that was encrypted with asymmetric algorithms (RSA). Alice can get the key from different places such as her personal device or USB. The encrypted file will be synchronised to the cloud storage provider automatically as illustrated in the following figure.


Encryption and Decryption Form

Bob's Public Key

Look In: Mardin

File Name:

Files of Type: All Files

Figure (6) Encryption and decryption form

IV. Evaluation

As in Kurdistan there is no cloud computing in e-health,a questionnaire is designed mainly for evaluating the application software that is intended to be installed in any healthcare team's personal device and sent to dropbox as a type of public cloud computing. Twenty participants took part in the questionnaire.

The questionnaire consists of three sections. First section relates to the participant's general knowledge about Cloud computing. The purpose of asking these questions is to know to which extent the participant can understand the application that depends to the knowledge that he knows.

The second section is about the usability of the application. We want to guarantee that the user can go through all the steps without needing to press the button 'Help'.

All the questions in this section wrote in a way that the user can give rating code between one to four (from strongly agree to disagree) to usability, consistency, familiarity with other application and efficiency.

The last section gives the opportunity to the participant to give their opinion about the application and how can be improved from their point of view.

Most of the participants agree that the application does as the title say and they have the same opinion of the flexibility of managing the encryption process and controlling the situation of generating the key. Furthermore they feel that their data is safe and no one can see the content of their documents which leads to become more comfortable toward using Cloud computing storage. They have the impression of using these kinds of applications with enhance the security level of Cloud storage.

The responses of the participants show that this application can provide the security that they can rely on. They mostly agree that being able to encrypt their data before sending it to Cloud and doing this process offline make them feel happy and more comfortable with this idea. The following is the result of the questionnaire

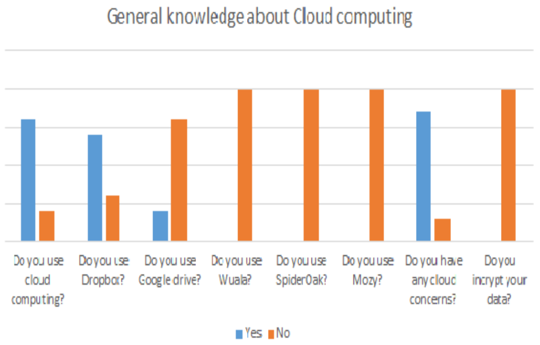


Figure (7) Participant's answers for section one

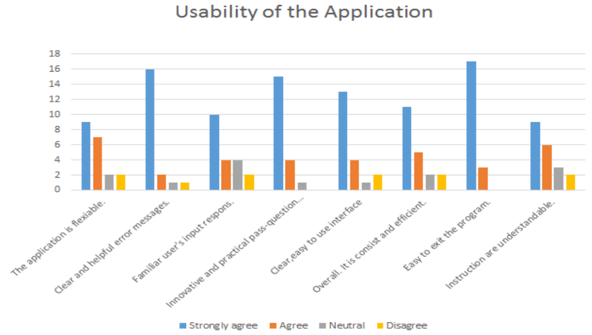


Figure (7) Participant's answers for section two

Figure (8) Participant's answers for section two

V. CONCLUSIONS & FUTURE APPROACHES

From the participants'responses we found that the participants believe that this application provide the security that they looking for. Moreover, the idea of having two-tier authentication will increase the security required in these kind of software.

This makes us believe that design user friendly interface has big impact on the user to use any kind of application. Additionally, knowing user's requirements and investigate the available solutions were important step to take in the beginning. Because these steps help in planning a better application and avoid the mistakes that the available solution have.

We suggest for future to still use two-tier authentication stages but with different ideas. Voice or image recognition can be used instead of security question. In voice recognition, we recommend that during the registration process, the user enter 5 words then in second tier authentication the user will recognise these word among other 5 word. Which means the user should select the entered word and pronounce it in the same time. Then the system will do voice match algorithm. If the result is greater that 70 then this is the real user otherwise access is denied.

References

[1] Thilakanathan, D., Chen S., Nepal S, Calvo R., Alem R, "A platform for secure monitoring and sharing of generic health data in the Cloud", Future Generation Computer Systems 35 (102–113), Elsevier, 2014.

[2] HealthTech, Wire Interview (05/04/2012). Data Sharing is the key to lower healthcare costs. EMC Corporation.

[3] Abdmeziem M., Tandjaoui D.," An end-to-end secure key management protocol for e-health applications" Computers and Electrical Engineering 44 (2015) 184–197,2015

[4] Heiser, J & Nicolett, M. (2008) "Assessing the Security Risks of Cloud Computing", Gartner, No. G00157782.

[5] Atayero, A. A. & Feyisetan, O. (2011) "Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", Journal of Emerging Trends in Computing and Information Sciences. Vol 2. No. 10.

[6] Chow, R. Golle, P. Jakobsson, M. Shi, E. Staddon, R.,& Molina, J. (2009) "Controlling data in the cloud: Outsourcing computation without outsourcing control", In ACM Workshop on Cloud Computing Security.

[7] Harauz, J. Kaufman, L. & Potter, B. (2009) "Data Security in the World of Cloud Computing", IEEE Security and Privacy , ISSN 1540-7993.

[8] Gens, F. (2008) "IT Cloud Services User Survey, pt.2: Top Benefits and Challenges". Enterprise IT in the Cloud Computing Era. IDC..

[9] Agrawal, V.K.& Dinesha, H.A. (2012) "Multi-level authentication technique for accessing cloud services", Computing, Communication and Applications (ICCCA), International Conference on, Vol. 10, No. 5, pp1-4.

[10] Agrawal, V.K.& Dinesha, H.A. (2012) "Multi-level authentication technique for accessing cloud services", Computing, Communication and Applications (ICCCA), International Conference on, Vol. 10, No. 5, pp1-4.

[11] Riedl B., Grascher V., Neubauer T.,"A Secure e-Health Architecture based on the

Appliance of Pseudonymization" JOURNAL OF SOFTWARE, VOL. 3, NO. 2, FEBRUARY, 2008

[12] Liu C., Huanga X., Liu J."Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption" Future Generation Computer Systems 52 (2015) 67–76, 2014