International Journal of Engineering, Science and Mathematics
Vol. 6 Issue 8, December 2017 (Special Issue)
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

END TO END ENCRYPTION BASED PRIVACY FOR MENTAL HEALTH CARE DATA TRANSACTION IN THE CLOUD

**Gangu Dharma Raju*
Adapa Chandrakala****
A V S Pawan Kumar*****
M Prudhvi Ravi Raja Reddy******

Abstract

*From the prevailing procedure of uploading information and transmission by the reasons of its reasonable cost, fast, global scale, efficiency, behavior, and reliability*the *Cloud computing is anextraordinary progress. The have no. of uses of cloud in the sector of education, social networking and medicine. But in medical the uses of cloud is ideal, particularly because the healthcare organizations data is produced very large. In cloud, as in increasingly health organizations adopting towards electronic health records which can be accessed around the world for different health problems regarding references, educational research in healthcare and etc. However, in the cloud data transferrable the privacy and security of data remain the demanding the problems. It is unavoidable which is stored and transferred using cloud to accept tight security to protect the integrity of the carefulmedical information, from the tampering attacks, hacking and intrusion. To secure communication from the third parties called opponent cryptography is the best practice of technique. In this paper, to protect mental health information we give an approach for which data could be in readable form to sender and receiver only by using End to end encryption technique such as a strong encryption method, also we propose a multi factor authentication to make sure data privacy which logging is followed by a user name and password then the person is to answer a question corresponding to the subject via OTP (One-Time-Pad). Once authentication is successfully verified a user can permit todata accessing in the encrypted method. After that, a user can use the key to decrypt the information and can use it for their purposes. According to the result of experimental the system has enhanced the confidentiality and data integrity greatly in the cloud.*

Keywords:

Cloud, Data Security,
Integrity, Confidentiality,
End to End Encryption,
Multi-Factor Authentication,
One-Time-Pad.

Author correspondence:

Gangu Dharma Raju,
Asst. Prof, Dept. of CSE, Baba Institute of Tech. & Sciences, Visakhapatnam, AP, India.

*Asst. Prof, Dept. of CSE, Baba Institute of Tech. & Sciences, Visakhapatnam, AP, India.
**Asst. Prof, Dept. of CSE, Baba Institute of Tech. & Sciences, Visakhapatnam, AP, India.
***Asst. Prof, Dept. of CSE, Baba Institute of Tech. & Sciences, Visakhapatnam, AP, India.
**** Asst. Prof, Dept. of CSE & IT, Aditya College of Engineering & Technology, E.G. Dist., AP, India.

1. Introduction

In the operational expertise the technologies in such industries are not used sufficiently, thus constrains the medical areas. Some medical areas is there which is still records are in paper. Likewise, those have computerized their data in healthcare areas. The adoption of technology will facilitate to collaboratein the essential of the healthcare sector to distributing the data simply between victims, physicians, doctors, psychiatrists and healthcare researchers. To convert and rebuilt the healthcare sector the cloud computing is adopted universally. The medical organization is transition into a paradigm which helps to altogether support and corresponding the workflows and medical data. Among authorized users and hospitals cloudcomputing facilitates to load large amount of information, and allow for data distributionalong with increasing the data analysis or tracking features. It will help toimprove the potential of doctors and to supply good treatment to the patients and also helps with reasonable cost to enhance researcher's data reference. In the healthcare organization, the extraordinary significance should be given to the security that is confidentiality, integrity, and availability of information to end users. The information must be with long-term protection, data traceability, and data reversibility. To data interchange, preserving, and using expansive informationin Information technology systems some challenges and issues faced by the medical organization. Therefore, a special attention should be given to organization clinical and nonclinical information while moving medical data into the cloud storage. The cloud deployment can be public, private, community or hybrid. The public cloud deployment model is used to store the non-clinical information. The people involved in the sector like medical practitioners, doctors, researchers and etc could handle with three leading cloud service paradigms that could address their occupational demandsThe encryption algorithm Tresorit applies is AES256 in CFB mode. Each file version gets a fresh, randomly chosen 128-bit IV in order to guarantee semantic security. Encryption keys of files and directories are changed from time to time, using a so-called "lazy re-encryption" pattern. This means that after the group's membership exchanges, the encryption key arerevive the next time a file's data change. This assurance that if you eliminate somebody from a group you distributed files with, they will not be able to decrypt any new data they did not have access to before remove their removal. In the meantime, you don't need to re-encrypt everything right away, saving computing resources and time. However, data encryption based on the Advanced Encryption Standard (AES) algorithm is very compute intensive. This type of software-based encryption depend on compute-intensive algorithms that can affect the behavior of the computing network, mainly the huge volumes of data that pass to and from the cloudwhen used pervasively to save. To create computinglogjams Conventional encryption solutions can be usedue to highly behavior overheads, for protecting cloud data trafficmaking them as less than optimal. At client side the Encryption and decryption processes are done. No one is able to access stored information, except for the owner and users authorized by the owner. No assurance in the cloud storage provider is necessary. So, in this paperfor overcoming the above described difficulties in the health care center weintroduce the novel end to end encryption based security establishment method.

2. Research Methodology

In this section discusses about the secure mental health care data transaction in cloud which is done by using the end to end encryption procedure along with the one-time pad based multifactor authentication procedure. The secure health care information transaction is done in both user side and hospital side in cloud environment which helps to eliminate the intermediate attacks. Then the basic architecture of the end to end encryption based secure mental health care information transaction is shown in the following figure 1. This secure medical health care information transaction of both doctor and patient side has been discussed as follows.

2.1. Transaction at Hospital Side

In this section discusses about the hospital side health care information transaction which is done with the help of the noise protocol framework. This frame work successfully encrypts the medical information because it utilizes the Diffie-hellman key agreement process which consists of single message along with the interactive protocol. The secure system uses the handshake messages which consist of static key patterns while the information transmission process. These patterns are arranged by collections of tokens which are helpful at the time of creating the handshake messages. Using cloud environment exchanged the created handshake messages i.e. while storing the data in the cloudthis exchangebetween the parties using public key. While transporting the created message or information in the cloud, the result of Diffie-Hellman operation will be shared with the help of sharing secret key. The shared noise message or hand shake message has 65536 bytes in length, the size of the message does not change because it has number ofadvantages such as simple testing, decrease the errors while dealing the memory and integer overflow, support to randomly access the decryption data and encapsulated with the higher level protocol. In addition to this, the noise

handshake message consists of Diffie-Hellman public keys that is arbitrate by own message patterns and zero-length plain text. Along with this, the transmitted medical information encrypts with the help of noise protocol frame work using three different functions such as DH function, cipher function and hash function.

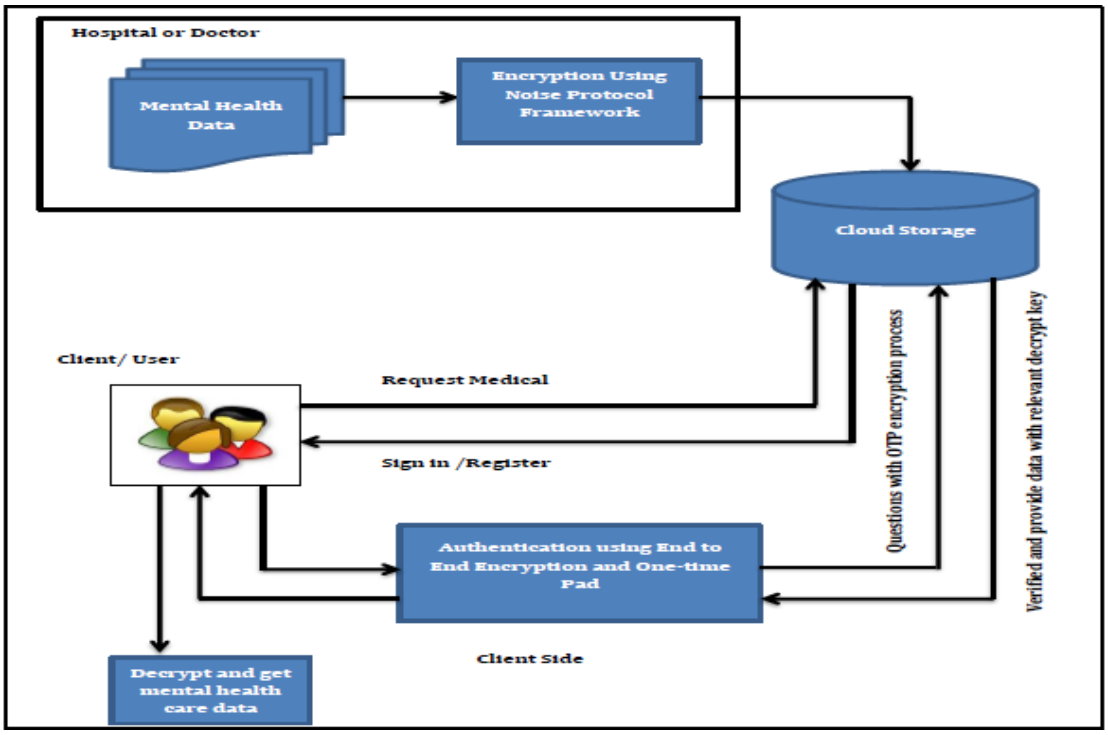


Figure 1 Mental Health Care Data Transaction using End to End Encryption based Secure

Initially the DH function has been created which consists of public key, private key. Generate_Keypair() is used for generating the DH function. The utilized public key helps to specify in the DH function which converts the bytes in to the DHLEN the output of the length must be greater than the 32. In this work, for making the DH function the AESGCM (Advance Encryption Standard Galois Counter Mode) has been used becausewhile exchanging the handshake messages it working effectively in parallel processing, easier implementation also pipeline instructions are successfully handled. The GCM process the messages using the symmetric key cryptographic approach that successfully encrypts the hand shake messages. Then the GCM based hash function is defined as follows,

$$GHASH(H,A,C)=X_{m+n+1} \quad (1)$$

In the above eqn (1), H is defined as the hash key, A represented as the shared medical data which need to be authenticated at the time of transmission, C is the cipher text, m is the number of bits. Then the output X_i is calculated as follows,

$$X_i = \begin{cases} (X_{i-1} \oplus A_i).H & for\ i = 1, \ldots . m-1 \\ (X_{m-1} \oplus (A_m^* \| 0^{128-v})).H & for\ i = m \\ (X_{i-1 \oplus} C_{i-m}).H & for\ i = m+1, \ldots . m+n-1 \end{cases} \quad (2)$$

In the above eqn (2), v represents as the bit length value of A. by using the above eqn (1 and 2) the shared health care information related DH function value or cipher text has been computed. In addition to this, noise message is determined with the help of the cipher function and hash function which helps to successfully encrypts health care information which is distributed in the cloud by exchanging the key values between the doctors and cloud storage provider.

While user requests the data access, the key detailsare provided to the user by the cloud provider. The hospital side data encryption process related algorithm step is discussed as follows.

Algorithm for health care information' Sharing in Doctor Side

Step 1: The keys used in the data exchanged are initializedsuch as public key, secret key.

Step 2: use hand shake messageexchange the public keys between the cloud storage provider and doctor's

side.

Step 3: The DH functions are created by noise message which is done by as follows,

$$GHASH(H, A, C) = X_{m+n+1}$$

$$X_i = \begin{cases} (X_{i-1} \oplus A_i).H & for\ i = 1, \ldots . m-1 \\ (X_{m-1} \oplus (A_m^* \| 0^{128-v})).H & for\ i = m \\ (X_{i-1 \oplus} C_{i-m}).H & for\ i = m+1, \ldots . m+n-1 \end{cases}$$

Step 4: According to the message transmissionvalue is varied.
Step 5: The calculated DH function output value will be hashed using secret key.
Step 6: At last the cipher text transmit in the cloud with relevant key values.

Based on the above algorithm steps are making the secure data storage the health care information has been transmitted in the cloud. The client accessed the transmitted data depending on the demands.

2.2. Transaction at Client Side

In this section discusses about the client side transaction while accessing the cloud health care information. Initially the user requests the cloud provider for accessing the particular health care information. The cloud provider wants to sign-in or sign-up their details for making the effective secure transaction. During this process, for ensuring the authentication between the cloud requester and cloud provider by using End to End encryption process along with the One Time Pad based algorithm. This authentication process further reduces the intermediate attacks and unauthorized access with effective manner. While user request for the particular medical data this secure encryption process works in both sign up and sign in process for every time. The security provides the end to end encryption process in both side also eliminates the intermediate attacks in terms of internet providers, telecom providers and so on. During this process, the messages are exchange between the parties to ensure the authenticated party which is done by using the Diffie-Hellman Key exchange process. Before that the authenticated parties are determined in terms of applying the One Time Pad (OTP).Cloud provider introduces the OTP pad to the user monitor which is available in particular time and the particular key word is sent to their phone number when the user registered their details along with the phone number into the cloud provider. While establishing the private communicationthe user wants to enter their number using the OTP pad which is available in screen that helps to ensure the authentication between the provider and user because it is so effective. Also ensures the freedom at the time association between the user expressions in cloud. To exchange the keys between the parties the OTP pad consists of collection of digits is used. Initially the user typed secret keys are converted into the digits which are transmitted to the cloud provider. The typed OTP values are matched with the provider secret key they are authenticated at first stage. Then the user request has been examined and the relevant key values are exchanged via the end to end encryption process to the authenticated user. The data has been accessed with relevant decryption keybased on the exchanged key values. Then the user accesses their requested related health care data successfully. Based on shared handshake messageby using the noise protocol framework the decryption process is further secured. Then client side secure data access process related algorithm step is explained as follows.

Algorithm for Health care information Accessing Client Side

Step 1: use sign up or sign in process of Request the cloud provider
Step 2:using the secret key which is received from phoneauthenticate the user
Step 3: using the OTP pad which is provided by the cloud provider enter the secret key
Step 4: exchange their key with cloud providerafter authentication,
Step 5: Then, for accessing the data with related decryption key the key values of DH are exchange.
Step 6: use therelevant secret key and handshake message for decrypt the data.

The above Health care information Accessing at Client Side the end to end encryption along with OTP based encryption process successfully authenticate

3. Results and Analysis

In this section discusses about for secure medical information storage in cloud environment the proposed noise framework protocol excellence along with end to end encryption process. In this work, for

making the psychological research in different fields of mental medical information has been stored. The data set consists of collection of data that is gathered from different peoples such as adults, young people, and children. Their health analyzed using those collected information, mental issues, and disorders and so on. For accessing those data's with easiest manner the mental health data need to be shared in the cloud. But the personal data must be managed from intermediate attacks and illegal access. For this purpose, to maintain the security the noise framework protocol along with end to end encryption process is used personally, validate privacy and confidence between the user and cloud provider with effective manner. Further the security is evaluated in the cloud environment with the help of the security, data uploading and authentication metrics. Then the utilized efficient metrics are listed as follows.

3.1. Privacy

Privacy is important metric which is used to encrypt the user personal information and health care data with their exchanging messages, keys and OTP secrete keys that help to hide the important data from the spammers.

3.2. InformationDistribution and Storing

At the time of data sharing, encrypt the health care information using their details public key along with the encryption method which is difficult to hack by the third parties.

3.3. Authentication

Using the end to end encryption process checks the authentication and authorization is done which only allows the matching users for accessing their information in the cloud server. In addition the method uses the secret key, access controls for maintaining the authentication with efficient manner. Then the proposed system achieves the less encryption time protection for user data which is shown in the figure 2.

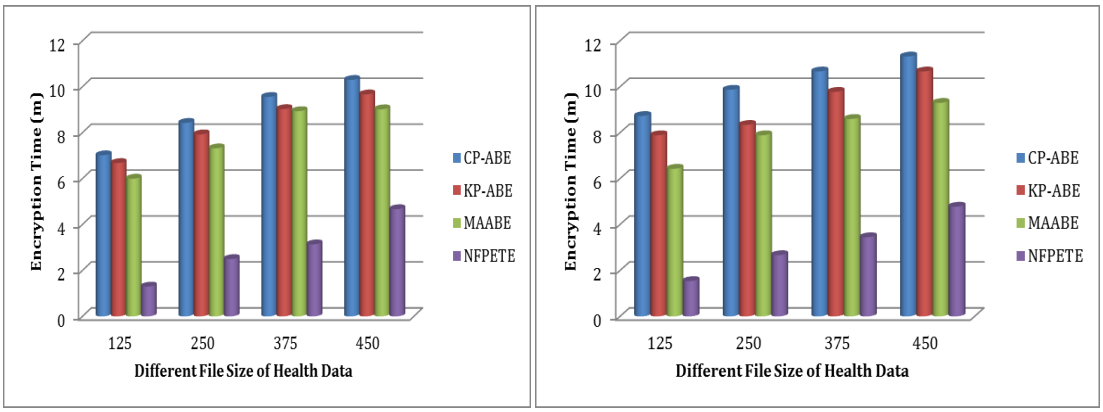
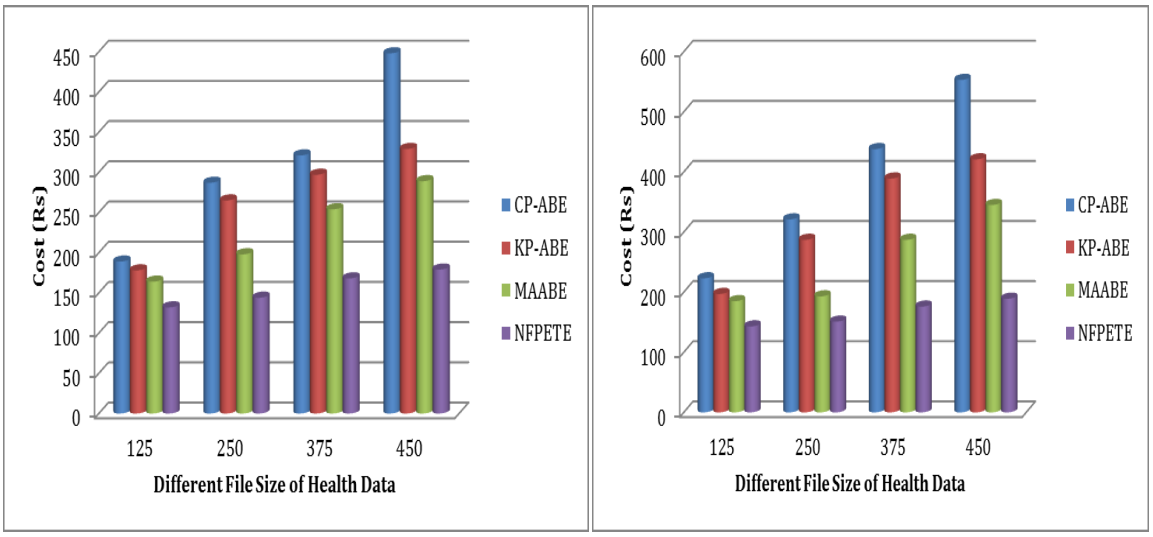


Figure 2 Time for Different Encryption Method a) APA dataset Cost and b) MHSDS dataset Cost

The above figure represents that the noise framework protocol with end to end encryption (NFPETE) method encryption time. The algorithm successfully encrypts the health care information with effective manner of different file size while doctor requesting the data uploading process in cloud. Then the proposed system reduce the encryption time due to efficient key interchanges and handshake message interchange procedure which leads to rise the security in the cloud efficient manner. The less encryption time enhances the overall execution time for both data sharing and security procedure in both dataframes.

The proposed system authorization access procedure and consumes less execution time for overall encrypting. The proposed system uses to improve the security with efficient manner when compared to the other methodsby the handshake message and OTP based authentication process. In additionwhile providing the security to the user information the system consumes minimum cost. The cost consumes for the system is shown in the figure 3.



(a) (b)

Figure 3 Cost for Different Encryption Method a) APA dataset Cost and b) MHSDS dataset Cost

The above figure represents that the proposed systemwhen compared to the existing methods it consumes minimum cost for different file size. Thus the proposed system when compared to the existing methods ensures the security with minimum time in the cloud environment. So, the user information is successfully managed in the third party server.

5. CONCLUSIONS

This paper discusses that the protected medical information storage in cloud using the noise framework protocol with end to end encryption along with OTP method. The method establishes the security for shared data in terms of both client side and doctor side. The method utilizes the DH function, handshake messages along with hash function during the authentication process which provides the authentication in doctor side. With the help of end to end encryption process the shared information has been accessed by the client. The data has been successfully stored and accessed via the cloud with effective manner based on the key sharing process. In additionwhile authenticating the user details the system uses the efficient key. Then the performance of the system is evaluated with the help of the Matlab tool in terms of the encryption time, execution time and cost.

References:

[1] Chase, M. and S.S. Chow, 2009. “Improving privacy and security in multi-authority attribute-based encryption,” in CCS, 121–130.

[2] Melissa Chase “Multi-authority Attribute based Encryption,” Computer Science Department Brown University Providence, RI 02912.

[3] Bethencourt, J., A. Sahai and B. Waters, 2007. “Cipher text-policy attribute-based encryption,” in IEEE S& P, 321–334.

[4] S. Narayan, M. Gagne´, and R. Safavi-Naini, “Privacy Preserving EHR System Using Attribute-Based Infrastructure,” Proc. ACM Cloud Computing Security Workshop (CCSW‟10), pp. 47-52, 2010.

[5] Ch. Padminiet. al. “Scalable and secure sharing of personal health Records in cloud computing using hhAttribute-based Encryption”, International Journal on Recent and Innovation Trends in Computing and Communication ISSN 2321 – 8169.Volume: 1 Issue: 8 679 – 681 AUG 2013.

[6] Shucheng Yu et. al. “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing” Proceeding of the 29th conference on Information communications pages 534-542, ACM, 2010.