International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 06, 2020
ISSN: 1475-7192

ENHANCING DATA SECURITY IN E-HEALTH CLOUD USING ATTRIBUTE-BASED ENCRYPTION, AES & STEGANOGRAPHY

Adwitiya Trivedi, Tushar Paliwal, Ramaprabha.J,Dr.S.Prabakaran

ABSTRACT*-In recent years, the growth in cloud computing has resulted in its application in multiple fields; one of them is E-Health Cloud. E-Health Cloud is the storage of the patient records in the cloud. The cost of services in health care is skyrocketing and professionals are to find, so the organizations have started adopting IT systems which helps them automate and streamline the process in a very cost-effective method. As the utilization diversifies, the amount of the data stored in the E cloud rapidly increases. Since the type of data in E-Health Cloud is sensitive, the privacy of data becomes a critical concern. This study explores the application of modern encryption techniques (AES and ABE) with steganography to study the storage, sharing and administration of medical data. Further, this paper will be used as a foundation to study techniques such as 3DES to compare with other encryptions and understand the advantages and limitations of each.*

Keywords – *E-health, security, AES, ABE, Steganography*.

I. INTRODUCTION

With the rapid advancements of cloud computing, health industries have adopted a faster way of storing and communicating the record of patients by using the E-Health cloud. Health industries use new technologies for sharing, storing, and managing the record of patients and electronic modes are used to support the fast delivery of health services. There are lots of privacy and security concerns which include confidentiality and multi-tenancy. Examples of other such concerns are- theft of data, Incomplete control over the accessibility of sensitive data, inability to monitor, inability to maintain regulatory compliance, outside provisioning(shadow IT). Multiple models were proposed to identify concerns of security and privacy like the data-sharing model, multi-level mechanisms and virtual domain encryption. E-records are of high importance as compared to MasterCard information as banks can easily cross out information of account holders to prevent security breach while records are difficult to destroy. The medical data needs a tight security as it contains the personal information of the patients and to share the data for future research the organization needs to be very careful not to leak sensitive information to the wrong people and to do that the organization needs a general data rule with the required policies while maintaining the confidentiality of data.

Received: 22 Feb 2020 | Revised: 13 Mar 2020 | Accepted: 05 Apr 2020

II. RELATED WORK

Many researchers have worked on enhancing the security of the E-Health cloud.

BABATUNDE, A.O.[1], TAIWO, A.J., DADA, E.G.[1] proposed a health care center using cryptography and steganography in which 3DES is used for encryption and the Least Significant Bit is used for steganography. Two main steps were taken to secure the patient data, the first step will take data in the format of text and will generate a 3DES cipher of it and a secret key will be required. The next step is to accept the output of the previous step and take it as input after that embed it one image which is also called cover image by using the least significant bit to obtain the output as stego.

The methodology improves security because of the two layers but the speed decreases significantly. Also since 3DES is used no rounds occur during encryption and the key length is fixed.

HUAQUN WANG[2] proposed model for sharing data is built from bilinear pairings. Bilinear pairings are derived from Weil pairings or Tate Pairings.

Initially, data is classified into various keywords and diff. types of data and the ciphertext list is generated (E1, E2, E3) and is uploaded to PCS.

PCS then sends queried data to sharers and data sharers decrypt data to get the plain text.

Yuan Zhang[3] proposed the first efficient and secure encrypted EMRs (Electronic Medical Records) deduplication scheme for cloud-assisted eHealth systems, and realize it in a system called HealthTap. In HealthDep, multiple dedicated key servers are introduced to assist in generating MLE keys, where these key servers share a secret via a distributed protocol and the MLE key is generated by the EMR itself and the secret jointly through an oblivious protocol. This guarantees that the confidentiality of outsourced EMRs cannot be violated by brute-force attackers when one or more key servers are compromised, and therefore, provides a stronger security guarantee compared with existing schemes.

They also analyze the medical data existing in actual eHealth systems. The key observation from the analysis is that patients consulting the doctors with the same department would generate numerous duplicate EMRs, while patients consulting the doctors with the different departments would generate few duplicate EMRs.

Mohammad Obaidur Rahman [4] proposed a system that uses E-LSB and cryptography, for the process of encryption an algorithm was used which is called Blowfish. The model had some advantages like it provided good PSNR values and the amount of data an image could hold was about 16KB.In this model, any format of the image was compressed

to JPEG format without any lossy decomposition. Though the issue with that is, if an unintentional attack happens that is reversing off the formats then the hidden data can be destroyed.

Aamer Nadeem[5] applied a few algorithms like DES, AES,3DES, AES(Rijndael) and Blowfish to check the performance and compared them by encrypting multiple files of various sizes. All the algorithms were implemented in a single language. They found out that Blowfish is one of the fastest algorithms but was not very secured for practice as the security/speed tradeoff was very high.

Received: 22 Feb 2020 | Revised: 13 Mar 2020 | Accepted: 05 Apr 2020

III. ALGORITHMS

AES is Advanced Encryption Standard is secure and a fast method of encrypting the data which keeps meddling eyes away. AES can be seen in apps like Whatsapp and other signal programs like WinZip and Veracrypt. Rijndael block cipher is used because of its abilities and ease of implementation in both software and hardware performance.

Working: Initially, data is divided into 4 blocks, the first thing what happens is that plaintext is divided into blocks and size if AES block is 128-bits, so data is separated in a 4 by 4 columns of 16 bytes.

Key expansion takes place as it involves taking a key and then using it with a series of other keys in every round during the encryption process.

New keys of the 128-bit round are used using Rijdael's key method. Now in each round, a key block is added using XOR cipher. The whole process is done in binary. In the substitution bytes process, every byte is substituted using a predetermined table. After that shifting rows and mixing columns is done. For decryption, we just apply the inverse of every step. Only theoretical breaks and channel attacks are uncovered by researchers.

ABE is a public-key encryption method in which the user who satisfies the access policy set by the admin will be able to decrypt the cipher. Policies will be defined using disjunctions and conjunctions and (p,q) -gates that are P out of Q attributes need to be present.

Key Policy is dual to CP-ABE that a policy is encoded into a key for example $(V \wedge Y) \vee Z$ and cipher are computed with attributes {V, X}. A very important property of ABE is called collusion resistance in which two different users would not be able to pool their secret keys to decrypt the ABE based ciphertext.

This is only one type of functional method of encryption, there are other methods like hidden vector encryption in which the encryption is done by vectorizing the attributes and inner product encryption.

IV. METHODOLOGY

The proposed system constitutes of 4 primary entities:

The data sharer: This is usually the doctor who is uploading the private patient information to the client. They are also responsible for setting the access policy of the data thus deciding the scope of data usage/access.

Authentication server: Performs the authentication of the current user accessing the system by issuing them a unique token upon every login. This token is utilized by other entities such as storage servers to obtain the attributes of the user, verifying their identities and obtaining the relevant parameters required for tasks such as key generation.

Storage server: The storage server is responsible for the storage and handling of encrypted data that is sent by the clients. It also performs the function of issuing decryption keys based on client attributes (which are again obtained through the use of access tokens). These keys are used by the client to decrypt the data that is retrieved from the server.

The data retriever: The data retriever uses their access token to verify their identity with the server and tries decrypt the data using the encryption keys received by them.

Process of encrypting files: The data sharer uses their credentials such as username/password to contact the authentication server to generate an access token.

Received: 22 Feb 2020 | Revised: 13 Mar 2020 | Accepted: 05 Apr 2020

Data sharer enters the data into the application and provides the appropriate access policy.

A random AES key is generated which is used to encrypt the plain text patient information data.

LSB Steganography is performed on the encrypted data and data is written onto an image.

Data sharer client application then requests the storage server for the CP-ABE public key using their access token. Using this CP-ABE public key the data sharer encrypts the random AES key and stores that into image meta-data. This image file is then sent to the server and stored on the file system.

Process of decrypting the file:-

The data retriever uses their credentials to sign in to the system and obtain a 2 access token from an authentication server.

They then contact the server along with their access token to obtain a CP-ABE decryption key that is generated using their attributes(which are obtained from their token by storage server).

A request is sent to the storage server along with their data retriever, and if the access token is verified then the requested file is sent back.

Then the retriever tries to decrypt the encrypted AES key embedded in image meta-data using their CP-ABE generated key.

If the access tree is satisfied, then they proceed with the decryption of the AES Key.

Once the AES key is decrypted, the data is ciphertext is then retrieved from the image and decrypted using this key.

V. RESULTS AND DISCUSSIONS

To evaluate the techniques and methods, average encryption and decryption times were recorded. Also, Peak Signal To Noise Ratio was calculated for four different file formats namely PNG, JPG, BMP and TIFF.

The below image shows the encryption time in seconds for different image formats using AES+ABE+LSB.

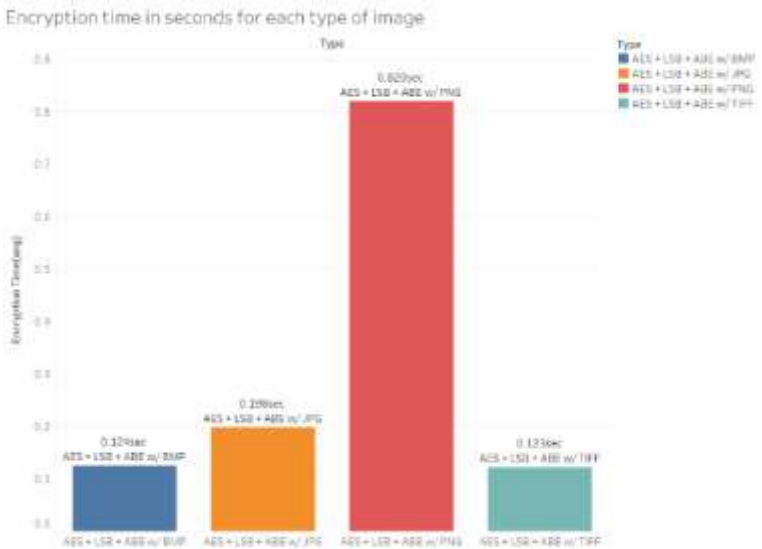

Figure 1: formats perform the worst among all

Here we can see that PNG image formats perform the worst among all the others while TIFF performs best during encryption followed by BMP and JPG respectively.

The below image shows the decryption time in seconds for different image formats using AES+ABE+LSB.

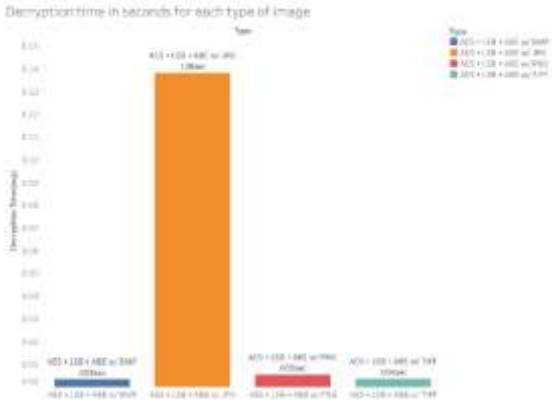

Figure 2: the others while PNG performs best

Here we can see that JPG image formats performs the worst among all the others while PNG performs best during encryption followed by BMP and TIFF respectively but the time taken to decrypt the file by JPG is less than 0.15 seconds which is not bad at all so we need to find the total time for each format in order to estimate which format works best with AES+ABE+LSB.

The below image shows the total time in seconds for different image formats using AES+ABE+LSB.

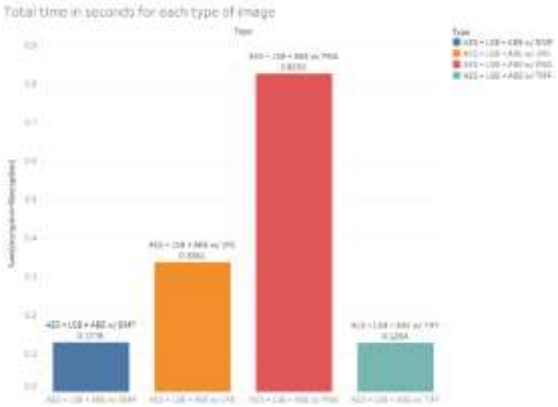

Figure 3: formats using AES+ABE+LSB.

In this figure, we can see that PNG takes the most amount of time as we know that the compression is lossless while BMP and TIFF perform best.

The below tables give us the Peak signal-to-noise ratio for various image formats when compared between the original and encrypted images.

PSNR VALUE FOR DIFFERENT FILE FORMATS

Sno	Format	PSNR value in DB
1	PNG	76.14138930506961
2	TIFF	76.17695825752641
3	BMP	76.06937117849564
4	JPG	41.457209994242525

Figure 4: the original and encrypted

After looking at this table we can see that JPG format is not at all suitable for the proposed model as it's SNR is maximum and MSE error is greater than any other format. Clearly, BMP and TIFF formats perform best during the total time taken in the process and also have a good PSNR ratio.

VI. CONCLUSION

The system provides the storage and transfer of E-health records and also overcome the security concerns with the introduction of Attribute-based Encryption in which the administrator can set the policies. The sensitive data is encrypted with AES and then that cipher is encrypted inside an image using steganography. A comprehensive performance-based comparison is also provided in the which shows that TIFF and BMP image formats perform best as compared to others.

REFERENCES

1. Information Security In Healthcare Center Using Cryptography and Steganography, BABATUNDE, TAIWO, DADA
2. Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-Health Record, HUAQUN WANG
3. HealthDep: An Efficient and Secure Deduplication Scheme for Cloud-Assisted eHealth Systems, Yuan Zhang, Chunxiang Xu, Hongwei Li, Kan Yang, Jianying Zhou, Xiaodong Lin
4. An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E LSB Encoding Technique Mohammad Obaidur Rahman†, Muhammad Kamal Hossen†*, Md. Golam Morsad†, Animesh Chandra Roy†, and Md. Shahnur Azad Chowdhury††.
5. A Performance Comparison of Data Encryption Algorithms. Aamer Nadeem, Dr. M. Younus Javed.
6. Cloud-Based E-Health Systems: Security and Privacy Challenges and Solutions, Mohanad Dawoud, D.Turgay Altilar
7. Cloud computing-enabled healthcare opportunities, issues, and applications: T A systematic review, Omar Alia, Anup Shresthaa, Jeffrey Soara, Samuel Fosso Wambab
8. Design and Implementation of Security in Healthcare Cloud Computing Molamoganyi Gorata, Adamu Murtala Zungeru, Mmoloki Mangwala, and Joseph Chuma
9. Time-Lapse Cryptography, Michael O. Rabin, Christopher Thorpe
10. Data Security and Authentication Using Steganography. Ravi Kumar, Murti