ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

CLOUD SECURITY USING BIOMETRIC ACCESS CONTROL AND WATERMARKED ECG

Latha.K*, and Sheela.T**
[1]Research scholar, Faculty of computer science and engineering, Sathyabama University, Chennai-600119.
Assistant Professor, Department of Computer Science and Engineering Sri Sairam Engineering College, Chennai – 600044.
[2]Professor & HOD, Dept of IT, Sri Sairam Engineering College, Chennai 600 044,Tamil Nadu, India.
Email: lathak.cse@sairam.edu.in

Received on: 03-02-2017 *Accepted on: 12-03-2017*

Abstract:

Electronic health record is the most tremendously growing sector in the past few years. The increase in accuracy and the capacity to handle huge amounts of data is crucial in making this grow faster and faster. The large amounts of sensitive data present in the cloud regarding patient's health details[3] and the accessibility given to them are the major security concerns involved with them. With the increase in technology in healthcare, various images such as x-rays, scan reports and various other images related to healthcare is present. These images that are stored in cloud need to be secure and retrieved only with proper authentication. Improper security with these data leads to data misuse and leakage of data. Poorly implemented health systems pose significant risk for patient safety and data misuse. The main security which concerns with the big data systems involve secure storage, secure access, and secure retrieval. In addition to strong access control mechanisms, location of data access is an important aspect of secure data usage. Recently reported incidents of illegal trade and stealing of patient data[5] over mobile devices remotely motivate research on secure data usage based on location. This paper deals with how these secure images can be retrieved using content based retrieval and also using biometric such as retina verification[22] and location based user authentication and using watermarked electro cardiogram signals(ECG).

Keywords: Privacy, Access control, Haar wavelet, Content based retrieval.

1. Introduction

Role based access control access to sensitive files cannot be given to everyone. Access to files depends on the person and their authority concerned. So role based access is the most basic way to secure data. The authentication of the user and his location form the vital parameters for this. In our approach, the health authority depends upon the validation of the mobile users depending upon the identity and location attributes. The role of the user, his

identification and location is verified. A mobile user which consults with the domain server, and forwards the request to the health authority. To manage EHRs efficiently and securely, we propose a design based on steganography, which we use to hide confidential EHR data inside the ECG host data. Steganography offers more efficient and secure information concealment than traditional cryptography. Only authorized users can extract data based on their security parameters. Our approach improves the security of storage and retrieval of EHRs by hiding them inside ECG signals, and enhances performance through flexible feature adoption (such as dynamic policy changes).

In a mobile service, location verification is also vital in distributing privacy-sensitive data[1]. Face biometrics can be used to provide authentication to a better extent. It also verifies the user in a domain. This also verifies the user location. Thus using these two parameters, the identification of the user can be validated. The health authority generates a key to each user using certificate-less public key cryptography. These keys are unique to each role played by the user. The role-based access control model maps generate these keys and controls them. The data and information retrieved is based on the keys entered by the user. The Kerberos Protocol is used to communicate the keys to the user in a secure protocol to avoid its misuse.

2. Kerberos Protocol: This protocol has two main parts:

1. The authentication server
2. Key granting server

The authentication server verifies the authentication of the person using the role they perform. Role hierarchy which classifies the various roles like nurses, doctors, staff, attenders and laboratory workers based on their need to access data is used. The authentication server and key granting server work in a way that they complement each other. The key granting server works with the authentication server by checking if its constraints are met. The constraints include role, location, identification etc. Once it is fulfilled, it generates the keys to the user based on this constraint. Once the user enters the key the host verifies the key and decrypts the data. This decrypted data is then accessed by the user. This helps in securing the data by preventing its misuse.

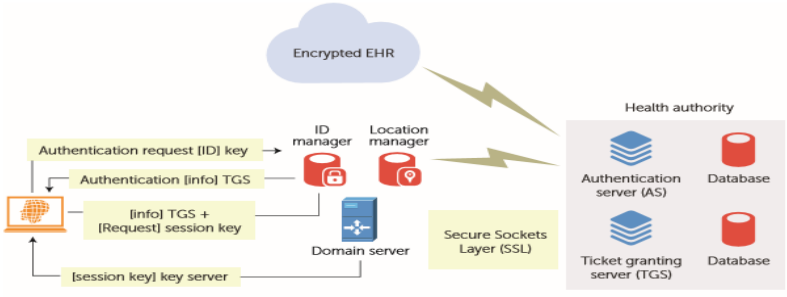

Figure 1. Architecture Diagram.

3. Retina Identification

What is important for an identification system is to be accurate, low cost, fast, and safe. Almost all current identification methods such as fingerprint, face, hand palm and iris recognition, are vulnerable considering plastic surgeries and some other changes in face, palm and finger print, while this is not the case for the retina. Human retina would never change and thus the uniqueness of the retina blood vessels pattern[23] is the most accurate pattern among other biometric systems. Here the method used for human identification of retina is using fuzzy c-means clustering algorithm[25]. This method is not sensitive to the rotation, rescaling and transformation. The features are Fourier-Mellin transform coefficients and moments of the retinal image. A rotation compensator was designed instead of the rotational effects of the retinal scanner.

The Haar wavelet[10] and snakes model have been used for the optic disc localization.

This method uses two main parts, feature extraction component and decision-making component. In feature extraction component, first vessels of the blood extracted and thinned by a morphological algorithm. Then, two feature vectors are constructed for each and every image, by using angular and radial partitioning. Manhattan distance[11] has been used as similarity measure between images. a fuzzy system with Manhattan distances of two feature vectors as input and similarity measure as output has been put in to the decision-making component. Simulations show that this system is about 99.75% accurate which makes it very useful in this security concern.

Pattern matching is a key point in all pattern-recognition algorithms. Searching image which is requested in database is one of the major significant work in image-based identification systems. Feature vectors of the query image and images in the database are compared to each other and nearest image is returned as a result. In this algorithms for pattern matching, various distance criterions have been used as similarity measure. similarity Manhattan distance and Euclidian distance[11] are two of the most important measures used until now. Also some systems have used weighted Manhattan and Euclidian distances as their similarity measures.In feature extraction section, in the proposed system, there are two feature vectors that have been extracted for each and every image by applying angular and radial partitioning. Using 1D Fourier transform to the feature vectors could eliminate rotation effects. And also we used Manhattan distance as similarity measure between images. So, compute Manhattan distance between the query image and all the images stored in database. Since we have two feature vectors, we have two Manhattan distances.

Angular partitioning may be better for some cases and radial partitioning is works better for some other cases. Angular partitioning gives 98% accuracy[26] and radial partitioning gives 91.5% accurate.

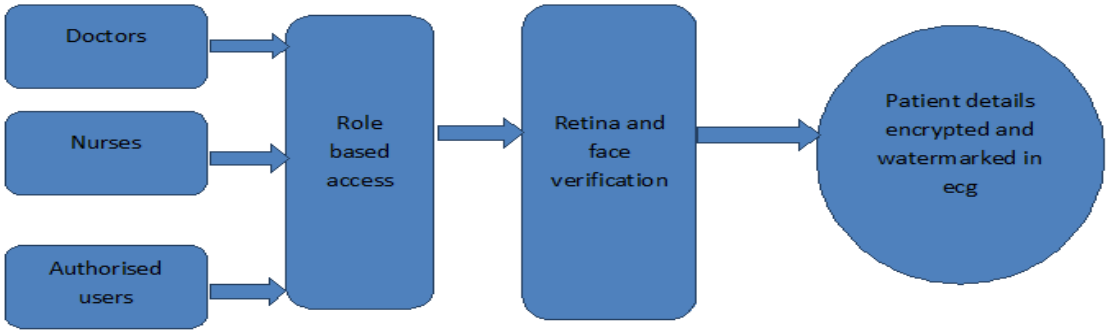

Figure 2. Working model.

4. Securing Data

The sensitive data of the patients is to be distributed and stored in the electro cardiogram(ecg) of the patient[6]. This helps us in achieving various levels of security in databy encrypting and the embedding it. This is done by replacing certain bits of the ecg with the patient data. Simple bit replacement can significantly hamper the ecg leading to loss of data. But this can lead to the original ecg being totally distorted. So, to minimise the distortion, we can apply wavelets[9]. When wavelet transformation is applied to the data, it is randomly split into many coefficients. These coefficients can then be randomly hidden in the least significant coefficients of the ecg thus reducing the amount of distortion. Thus here the data is organised into a tree structure and data is randomly encrypted.

The medical data that is to be stored is first organised based on its contents into a tree structure. Then based on their indexes(I) and ends(E) it is allocated to different parts of the ecg randomly. The ecg is then split and haar wavelet transformation[10] is applied on it. The main purpose of applying wavelets is to avoid the distortion problem. Applying this haar wavelet[10] on the ecg yields two sets of coefficients called coefficients approximation(CA) and coefficients detailed(CD). These coefficients denote the most sensitive feature of the ecg. CA is defined as the most sensitive features and CD is defined as the least significant features. For each section in the data, a hash value is computed for the data. A security key is devised for each patient to make the hiding process unique. This security key is used to encrypt the data and then the encrypted data is shuffled and hidden in a set of CD coefficients (least significant) and hide section bits in a certain set of coefficients. Then haar wavelet recomposition on both CA and CD. Then a new watermarked segment is reconstructed. Then the water mark and the shuffled, encrypted data is re-embedded into the full original ECG signal using its index and end. The same process is repeated for all the sections. Then the cloud stores all the data such as the indexes and ends, the hidden section number and key, along with a unique patient ID, which is vital for retrieval of the patient information. The health authority stores the watermarked ECG along with the generated number mapped to the patient ID on its cloud servers. Therefore, even if this

information is intercepted, it won't reveal anything. Thus it provides multiple layers of security beginning from the biometric and role authentication, key generation and at last the ecg encryption and embedding.

Figure 3. Haar Wavelet Transformation.

5. Working

The data is placed on the ecg. This data is then split and Haar wavelet[10] is applied to it to avoid distortion. Then these bits are again embedded into the ecg of the patient. The user has to then verify his authentication using face, retina and role authentication. Once they are verified, a key is generated by the key granting server. This unique key is used to access the data from the ecg. The key encrypts the data from the ecg and provides them to the secure user. Thus, the data is retrieved securely.

6. Image Retrieval

The processes involved in image retrieval are:

1. The user first has to authorise his role to the server which is then verified.
2. Then the user has to undergo a retina scan for authentication.
3. If both the parameters are verified and found to be authentic, then the ecg which contains the sensitive data is retrieved.

The role based authentication, does not allow unauthorised users to access the data. Then the retina test is very vital to make sure that the person is genuine. If both the parameters are satisfied, then the patient details can be retrieved using the patient id and unique key.

7. Conclusion

This process is found to be effective, though the major concern is the retina test. Retina test is expensive and may take some time. It is also expensive when compared to the other biometric tests. The embedding of the data in the ecg may also lead to lossy ecg image. If these limitations are overcome, then the process is highly effective and can be useful in protecting the sensitive data of patients.

References

1. Rui Li, Alex X. Liu, Ann L. Wang, and Bezawada Bruhadeshwar ”Fast and Scalable Range Query Processing With Strong Privacy Protection for Cloud Computing” in IEEE/ACM Transactions on networking, vol. 24,no. 4, august 2016
2. Zhihua Xia, Member, IEEE, Xinhui Wang, Liangao Zhang, Zhan Qin, Member, IEEE, Xingming Sun, Senior Member, IEEE, and Kui Ren, Fellow, IEEE “A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing” in IEEE transactions on information forensics and security, vol. 11, no. 11, november 2016
3. AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health Cloud: Opportunities and Threats. J. Network and Computer Applications 35 (1), 211-220.
4. Alvarez, R. (2004). The Electronic Health Record: A Leap Forward in Patient Safety. Healthcare Papers, 33-36.
5. Amatayakul, M. (1999). EHRs and the Consumer: A New Opportunity. In Murphy GF, Hanken MA, Waters KA eds, 26-68.
6. X. Liang, M. Barua, R. Lu, X. Lin, and X. S. Shen, “Healthshare:Achieving secure and privacy-preserving health information sharing through health social networks,” Computer Communications, vol. 35,no. 15, pp. 1910–1920, 2012.
7. R. Zhang, Y. Zhang, J. Sun, and G. Yan, “Fine-grained private matching for proximity-based mobile social networking,” in INFOCOM, 2012 Proceedings IEEE. IEEE, 2012, pp. 1969–1977.
8. Amir Said and William A. Pearman, 1996. An Image Multiresolution Representation For Lossless And Lossy Compression. IEEE Transactions on Image Processing, 5: 1303-1310.
9. Sonja Grgic, Mislav Grgic, Member, 2001. IEEE and Branka Zovko-Cihlar, Member, IEEE. Performance Analysis of Image Compression Using Wavelets. IEEE Trans., Vol: 48.
10. Anuj Bhardwaj and Rashid Ali, Image compression using Modified Fast Haar Wavelet Transform, Department of Mathematics, Vishveshwarya Institute of Engineering and Technology, Dadri, G. B. Nagar-203207, U.P. India
11. Deepak sinwar and Rahul Kaushik, Study of Euclidean and Manhattan Distance Metrics using Simple K-Means Clustering in international journal for research in applied scienc e and engineering technolo gy (ijras et).
12. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Advances in Cryptology–EUROCRYPT. Berlin, Germany: Springer, 2004, pp. 506–522.

13. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy, May 2000,pp. 44–55.
14. E.-J. Goh et al., "Secure indexes," in Proc. IACR Cryptol. ePrint Arch.,2003, p. 216.
15. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient onstructions," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 79–88.
16. J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," J. Internet Technol., vol. 16, no. 1, pp. 171–178, 2015.
17. M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in Proc. IEEE 28th Int. Conf. Data Eng., Apr. 2012, pp. 1156–1167.
18. C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in Proc. IEEE INFOCOM, Mar. 2012, pp. 451–459.
19. Z. Xia, Y. Zhu, X. Sun, and L. Chen, "Secure semantic expansion based search over encrypted cloud data supporting similarity ranking," J. Cloud Comput., vol. 3, no. 1, pp. 1–11, 2014.
20. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans.Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.
21. Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans. Commun., vol. 98, no. 1, pp. 190–200, 2015.
22. Tabatabaee H, Milani Fard A, Jafariani H: A novel human identifier system using retina image and fuzzy clustering approach. In Proceedings of the 2nd IEEE International Conference on Information and Communication Technologies (ICTTA '06). Damascus, Syria; 2006:1031-1036.
23. Xu ZW, Guo XX, Hu XY, Cheng X: The blood vessel recognition of ocular fundus. In Proceedings of the 4th International Conference on Machine Learning and Cybernetics (ICMLC '05). Guangzhou, China; 2005:4493-4498.Google Scholar
24. Ortega M, Marino C, Penedo MG, Blanco M, Gonzalez F: Biometric authentication using digital retinal images. In Proceedings of the 5th WSEAS International Conference on Applied Computer Science (ACOS '06). Hangzhou, China; 2006:422-427.

25. BEZDEK, J., DAVENPORT, J., HATHAWAY, R., and GLYNN, T. (1985), "A Comparison of the Fuzzy c-Means and EM Algorithms on Mixture Distributions with Different Levels of Component Overlapping," in The Proceedings of the 1985 IEEE Workshop on Languages for Automation: Cognitive Aspects in Information Processing, ed. S. K. Chang, Silver Spring, Maryland: Institute of Electrical and Electronic Engineers Computer Society Press, 98–102.
26. BEZDEK, J., HATHAWAY, R., SABIN, M., and TUCKER, W. (1987), "Convergence Theory for Fuzzy c-Means: Counterexamples and Repairs,"Institute of Electrical and Electronic Engineers Transactions on Systems, Man and Cybernetics, 17, 873–877.
27. DAVENPORT, J., BEZDEK, J., and HATHAWAY, R. (1988), "Parameter Estimation for a Mixture of Distributions Using Fuzzy c-Means and Constrained Wolfe Algorithms,"Journal of Computers and Mathematics with Applications, 15, 819–828.
28. DUNN, J. (1973), "A Fuzzy Relative of the ISODATA Process and Its Use in Detecting Compact, Well-Separated Clusters,"Journal of Cybernetics, 3, 32–57.
29. Reeja S L, RBAC in CLOUD COMPUTING USING CSAR ", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 10, October 2012.