A MEDICAL HEALTH CARE SYSTEM WITH HIGH SECURITY USING ANDROID APPLICATION

Mr. T.CHANDRA SEKHAR RAO
PROFESSOR and HEAD

T.SREEDHAR
M.TECH

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
LOYOLA INSTITUTE OF TECHNOLOGY AND MANAGEMENT , SATTENAPALLI,
ANDHRA PRADESH, INDIA-522412

ABSTRACT

A medical health care system with high security using android application is important in present life it deals with new algorithms and techniques i.e. multiphase encryption algorithms. In this algorithm we will encrypt and decrypt the value with different keys i.e. (k1,k2,k3…….kn). when it takes the value from the patient it will encrypt the value with three different keys. So that the value stored in the server very securely. When the doctor want to check the date it will again decrypt with three different keys the Value and sent to the android device which is connected to the established network. Doctor when connected to the local network he/she get the decryption values. So there is no scope of even hacking the network by the hacker to change the values sent to the server. So Patient life will be 100% secure from the attack.

KEYWORDS

Health care application, android device, multiphase encryption, health condition.

I.INTRODUCTION

INFORMATION and communication technologies are one of the most promising applications of information technology is healthcare and wellness management. Healthcare is moving from an approach based on the reactive responses to acute conditions to a proactive approach characterized by early detection, prevention, and long-term management of health conditions. The current trend places an emphasis on the monitoring of health conditions and the management of wellness as significant contributors to individual healthcare and wellbeing. This is particularly important in developed countries with a significant aging population, where information technology can significantly improve the management of chronic conditions and thereby improve quality of life.

For example, continuous recording of an electrocardiogram (ECG) or photoplethysmogram (PPG) by a wearable sensor can provide a realistic view of the heart condition of a patient during normal daily routines, and can help detect such conditions as high blood pressure, stress anxiety, diabetes, and depression. In addition, it is conceivable that further automated analysis of recorded biomedical signals could support doctors in their daily practices and allow the development of warning systems. This would bring several benefits: it would increase the health observability, collaboration among doctors, and doctor-to-patient efficiency and thereby decrease healthcare costs.

Recent technological advances in M2M systems together with the rise of M2M communications over wired and wireless links allow the design of lightweight, low-power sensors at low cost for wearable sensor networks, integrated circuits, and wireless communication With advances in mobile communication, new opportunities have opened up for

the development of healthcare systems that remotely monitor biomedical signals from patients. The availability of a new generation of mobile phones has had an important impact on the development of such healthcare systems, as they seamlessly integrate with a wide variety of networks (such as 3G, Bluetooth, wireless LAN, WCDMA and GSM), and thus enable the transmission of recorded biomedical signals to doctors or patients from a central server located in a hospital, home, or office. A smartphone presents a programmable monitoring platform for healthcare as people go about their daily lives.

The basic principle of Cryptography is defined as: A message being sent is known as plaintext. The message is then coded using a cryptographic algorithm. This process is called encryption. An encrypted message is known as ciphertext, and is turned back into plaintext by the process of decryption . The method for decryption is the same as that for encryption but in reverse direction. It is applicable in each phase of encryption. Multiple encryptions is the process of encrypting an already encrypted message one or more times, either using the same or a different algorithm. Under the same key length and for the same size of the processed data.

This paper presents a secure medical health care system using android. the use secure in the system is to protect the patients life. The data is stored in secure format so that no other person can steel the data.now you can understand by seeing the system design and the algorithm described below.

II.SYSTEM DESIGN

The overall architecture of a secure medical health care system is understand by using a diagram of flowchart and the system architecture. firstly the patient is connected with the ppg sensor to the hand so that a continuous reading is taken from the patient and it is sent to the gate way. The data which was taken is stored in the server it will maintain the record values of the all the patients. The doctor who was in the other place should have an android mobile device an app which was already developed was installed in the android mobile device. now doctor has to connect to the server in order to retrieve the information so that he will connect to local Wi-Fi which is present in the hospital in this the ip number has to maintained very securely other wise there is a chance of connecting to the network for other users. when he gets connected the data present in the server will sent in to the mobile device so that the doctor can see whether he was in serious condition or in normal condition. Not only he will monitor one patient he can monitor many other patient life. So there is secure health care system is built in the hospital.

Now we will see the flow chat diagram of data processing in figure 1 and system architecture in figure 2 below.

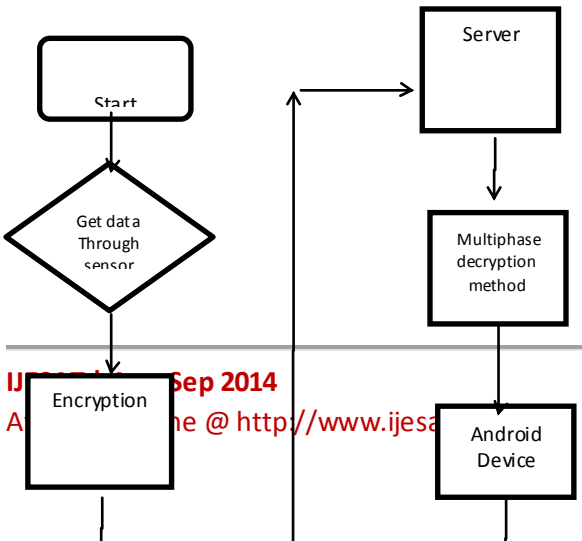

Fig 1: flow chart for data processing in the server

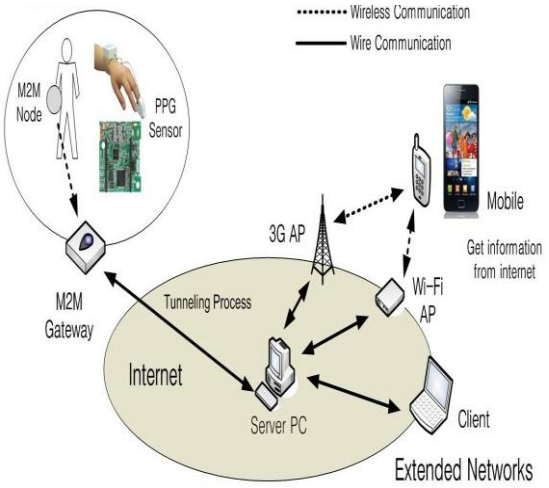

Fig 2: system architecture of secure health care system

So from the above flow char and system diagram we can easily understood we can provide a secure health care system. In the above at the gate way we use to encrypt the data which was taken from the patient and stored in the server, after if the doctor want to see the data store in the server he will connect to the server so that the data will decrypt and sent to the mobile device securely.

III.ALGORITHM

The algorithm which is used in the system is strong encryption and decryption algorithm. Now you can easily understood the algorithm how it going to work. First it will take the data which is going to store in the server. It will encrypt the data with k1 key so that the plain text is going to change in to cipher text and we will take again the cipher text and it is again encrypt with k2 key value a different value and lastly we will encrypt with k3 key value. So that we will get a secure cipher text which is not understand to even to the hacker. In the same manner again we will decrypt the data with three key values in order to get the original value. We can understand by seeing it below clearly

The encryption algorithm is:
cipher text = *EK*3(*EK*2(*EK*1(plaintext))) I.e., encrypts with *K*1, *decrypt* with *K*2, then encrypt with *K*3.
Decryption is the reverse:
plaintext = *DK*1(*DK*2(*DK*3(cipher text))) I.e., decrypt with *K*3, *encrypt* with *K*2, then decrypt with k1.

IV.EXPERIMENTAL RESULTS

Final from the decrypted data we will get the original information which can be seen in android mobile device. an android app which was developed in the android emulator should be present in the mobile device. so that the patient information in the plain text is sent in to the android mobile device. so which the doctor can monitor the patient health is safe or emergence condition.

In this two major things has to observe i.e. the graph is low frequency the patient is in normal condition if the patient result is high frequency the patient is in serious condition .now with help of small figure we can easily understand.

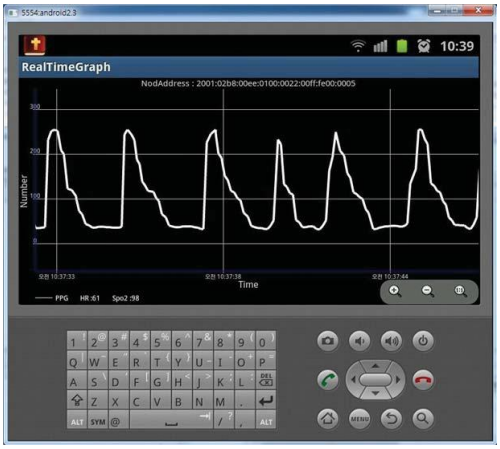

Fig 3: Android emulator test for the monitoring program on the server

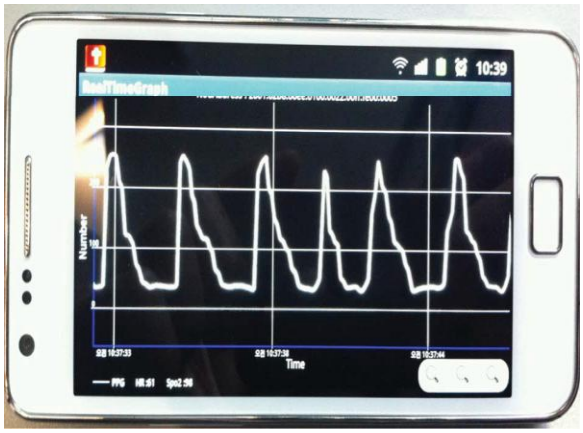

Fig 4: Appearance of the android mobile during monitoring

V.CONCLUSION

Finally successfully implemented a medial health care system with high security using android application with help of secure multiphase algorithm in which I have used different keys to protect the data from theft. And with the help of android device we can monitor patient health.

VI. REFERENCES

[1] G. Z. Yang, *Body Sensor Networks*, 1st ed. London: Springer-Verlag, 2006, pp. 1–275.
[2] P. S. Pandian, K. Mohanavelu, K. P. Safeer, T. M. Kotresh, D. T. Shakunthala, P. Gopal, and V. C. Padaki, "Smart vest: Wearable multiparameter remote physiological monitoring system," *Med. Eng. Phys.*, vol. 30, no. 4, pp. 466–477, May 2008.
[3] T. Yilmaz, R. Foster, and Y. Hao, "Detecting vital signs with wearable wireless sensors," *Sensors*, vol. 10, no. 12, pp. 10837–10862, Dec. 2010.
[4] B. Massot, N. Baltenneck, C. Gehin, A. Dittmar, and E. McAdams, "EmoSense: An ambulatory device for the assessment of ANS activityapplication in the objective evaluation of stress with the blind," *IEEE Sensors J.*, vol. 12, no. 3, pp. 543–551, Mar. 2012.
[5] Y. T. Chen, I. C. Hung, M. W. Huang, C. J. Hou, and K. S. Cheng, "Physiological signal analysis for patients with depression," in *Proc. 4th Int. Conf. Biomed. Eng. Informat.*, Shanghai, China, 2011, pp. 805–808.
[6] T. Taleb, D. Bottazzi, and N. Nasser, "A novel middleware solution to improve ubiquitous healthcare systems aided by affective information," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 2, pp. 335–349, Mar. 2010.
[7] J. G. Ko, C. Y. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, and M. Welsh, "Wireless sensor networks for healthcare," *Proc. IEEE*, vol. 98, no. 11, pp. 1947–1960, Nov. 2010.
[8] Y.Wang and M. Hu, ―Timing - evaluation of the known cryptographic algorithms,‖ in *proc. International Conference on Computational Intelligence and Security*, Beijing, China Dec 2009.
[9] R. Bose, *Information Theory, Coding and Cryptography*, Second Re1print 2008, the Tata McGraw Hill Publication, pp. 313.

ISSN: 2250-3676
Volume-4, Issue-4, 318-322