IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Review of Computer Engineering Studies
Vol. 7, No. 3, September, 2020, pp. 74-78
Journal homepage: http://iieta.org/journals/rces

Secure Online Medicine Delivery System

Mohammad Waqar Bhat, Veerabhadrappa Sondekere Thippeswamy*, Himanshu Bhushan, Kartik Shrivastava, Ashish Kumar Sahoo

Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bengaluru 560060, India

Corresponding Author Email: veerabhadrappast@jssateb.ac.in

https://doi.org/10.18280/rces.070305

Received: 10 July 2020
Accepted: 28 August 2020

Keywords:
telemedicine, online delivery, Advanced Encryption Standard (AES), biometric, pharmacy, telecare medicine information systems (TMIS)

ABSTRACT

The objective of this study to design and implement a secured home delivery of medicine to the specific customer**.** It also provides the time and effort exerted by the staff and ensures the accuracy of the patient's internal medical disbursement as well as the control of the disbursed quantities. Currently, the systems used in the telecare medicine information system for delivery purposes include the storage of information of the users in the remote server and involve various methods for authentication purposes at the client end. However, these systems are susceptible to uniqueness theft, guessing passwords, services denial, and implementation and insider attacks. This can be achieved by securing demographic information like name, date of birth, or the age of a person and also includes biometric ids given by the clients to the administrator. Furthermore, this paper provides a step by step Advanced Encryption techniques (AES) to enhance the security features by another layer. The data acquired from the user is processed through these encryption techniques and then finally stored in a Relational Database which is formed by using My SQL PHP admin. The Database stores all information related to the patient, admin, and medicine inventory. The overall idea is to create a smart and secure online based medicine delivery system that will find its application in the field of e-commerce vendors such as Practo, 1mg, Netmeds, etc. It shall not be possible to locate the client's consignment (medicine orders) based on the virtual IDs alone, rather a biometric verification will be carried out at the client's (patient's) end to confirm the authenticity from the client.

1. INTRODUCTION

Health-care delivery applications need a robust and secure medicine providing system [1, 2]. Telecare medicine information systems being a very important part of this digital era. Numerous low-cost telecommunication systems and monitoring equipment are present for the patients. Implementing the pharmacy application and integrated it with data getting from the existing systems, could help to increase the accuracy and ease of the creation of medical needs and stock management. Besides, it will decrease the number of medical supply stock-outs [3]. By using these systems the benefits of telehealth are made available to the patients at their homes. In these systems, the number of users is connected with numerous types of wired or wireless networks which makes this system prone to attacks by hackers. To avoid this, confirmation at both ends has become essential. The server at the host side needs verification to safeguard the records of the patient from an unlicensed person to protect the confidentiality of the patient, while on the other side, the patient (client) has to be authenticated by the host server so he/she cannot be impersonated by the hacker. A confirmation plan can keep unapproved clients from getting to medication data frameworks. The new advancement in the area of services and computing offers to deliver hosted services over the worldwide using public or private online cloud services [4, 5]. The idea of cloud computing can be established in many levels of implementation based on the type of problem. The use of new technologies like cloud computing and soft computing in analyzing the data of any system can help to understand the behavior of current and future data [6, 7]. In 1981, Lamport [8] introduced the primary verification conspire to utilize the secret key table and hash chain. As a secret key can be carefully chosen uninhibitedly by the client, secret word validation plans are broadly utilized in different applications [9-11]. A secret phrase can be undermined in certain situations. For instance, recorded by a government operative programming, shoulder surfing through a remote camera, reacting to a phishing email, taken secret word table from the hacked server, and so forth. When the secret word is uncovered, the validation plot utilizing the secret key alone is broken. Pertinent client confirmations plans are by and large used to take care of this sort of issue in TMIS because these conventions are viewed as the essential protects in organize electronic applications. Validation plans can guarantee that the framework's assets are not gotten deceitfully by illicit clients. Secret key based client confirmation plot is one of the least difficult and most helpful validation systems in focusing on insecure systems. It gives just the legitimate patients to use the benefits of remote frameworks. Many Internet applications are dependent on a secret key based verification plans, for instance, remote login, private companies, database the executive's frameworks, educational systems, etc. Most likely it is reasonable for the TMIS. In any case, the present Internet condition is defenseless against different assaults, for example, replay assaults, on-line and disconnected secret phrase speculating assaults, adjustment assaults, and taken verifier assaults. Henceforth, a solid confirmation plot is required

among clients and servers [12].

In another method, the proposed client validation system utilizes three sorts of cryptographic, scientific strategies and hypotheses, to be specific hash work, symmetric cryptography, discrete algorithm issue, flexible length, and the hash function being of a fixed length [12, 13]. In symmetric cryptography, session key assumes a significant job in the symmetric cryptography that in the way of symmetric cryptography, both communication parts, a customer and a server, share a session key. While correspondence is executed and the sending party utilizes a different way to encode messages transmitted over the web. The discrete logarithm is major to various open key calculations, including Diffie-Hellman key trades, computerized signature calculations, etc. the secret phrase-based client validation plot is proposed for the telecare prescription data framework. Secure Privacy-Preserving Biometric Authentication Scheme for Telecare Medicine Information Systems [14] considers the new security issues: personality namelessness and secure transmission in biometric verification conspire for TMIS.

1.1 Use of biometrics for identification

Using a biometric feature as key in a cryptographic process adds additional security to the system. It ensures the physical presence of authenticated users as it uses unique traits and is secure because of its universality. One such method was proposed using a fuzzy commitment scheme [15].

The use of fingerprints has been for security purposes for many years. A fingerprint is unique and this uniqueness depends on the various minutia points. For using the fingerprint data for security purposes the minutia from the fingerprint images must be obtained. However, the quality of the fingerprint image obtained from the fingerprint scanner depends on various external factors like variations in skin, moisture, etc. hence before the extraction of minutia, the images have to be enhanced to obtain more dependable minutia locations [16].

A fingerprint is mainly composed of furrows and ridges. These furrows and ridges present a significant amount to the similarity in a small local window. However, the fingerprints cannot be differentiated by the ridges and furrows but by minutia points which a point on the ridges. Instead, the set of two different types of points are considered while extraction of minutia points. These include ridges endings and bifurcations.

Ridge ends are the points where the ridge curve terminates and where ridge separates to two different paths at a Y junction is a bifurcation. Figure 1 illustrates an example of a ridge ending and a bifurcation.

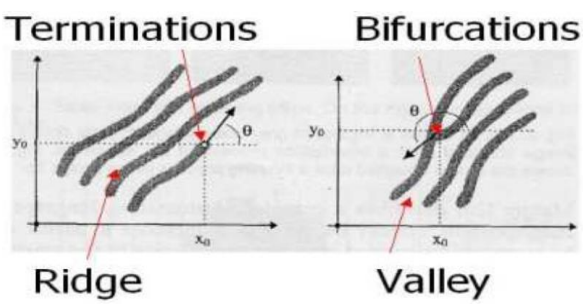

Figure 1. Ridges and valleys of fingerprint

In the following example above, the black pixels are the ridges, and the white pixels are the valleys.

2. SYSTEM DESIGN AND METHODOLOGY

The block diagram of the overall system is shown in Figure 2. The system consists of a microcontroller, server, and R307 fingerprint scanner, to both, acquire biometric data at the sender side and authenticate the receiver at the client-side. The R307 is an optical fingerprint sensor and its dimension is small in size and is integrated with its own DSP chip. It has very low power consumption. It can store up to 1000 fingerprints. The basic block diagram is shown in Figure 2. The Arduino microcontroller is used to interface the fingerprint sensor to the server so that the biometric data obtained can be stored in the server for authentication purposes.

Figure 2. Block diagram of the system

The online medicine ordering system in both the sender and client end is as shown in Figure 3 and Figure 4 respectively. The sender collecting the information of the patient, such as KYC, biometric data, and stored in the server. The delivery box containing the appropriate medicines is sent to the registered client on the basis of biometric authentication. Only after the authentication/verification is successful from the client's side, medicines are supposed to be delivered.

From the client's end when the box is received, biometric authentication is carried out which is encrypted based on Advanced Encryption Standard (AES), and this information is sent to the sender to verify the biometrics already present in the database. The sender authenticates the client and henceforth the medicine is delivered to the respective client.

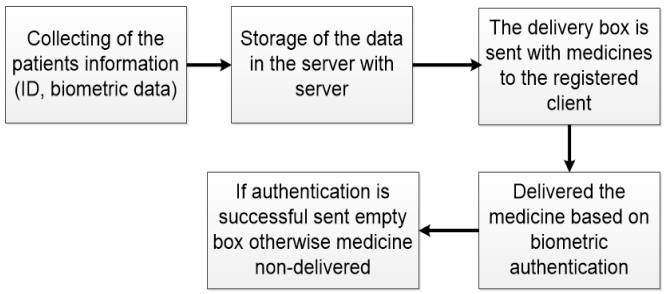

Figure 3. Steps followed at the sender

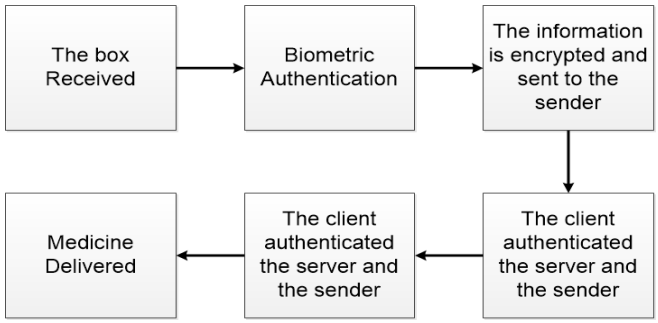

Figure 4. Block diagram of the system at the client

3. PROPOSED ALGORITHM

3.1 Advanced encryption standard

Advanced encryption standards (AES) [17, 18] is one of the most commonly used cryptographic methods for securing sensitive information. It uses a block cipher algorithm to ensure that data can be stored securely.

In the proposed method, Jorg and Buchholz's cipher is utilized and being used for the implementation of AES.

(i) It makes use of a password as the plain text. The password is 16 bytes transformed for the encryption and decryption algorithm.

(ii) The key is generated using the minutia points obtained from the biometric fingerprint. The key is also of 16-byte length. The AES initialization function is shown in Figure 5 [19].

(iii) The AES_init module has several sub-components like s_box and inverse s_box generation. RCON generation function is used for the key extension.

(iv) In the (10 x 4) matrix generated, the first column contains an 8-bit binary presentation of the power of 2.

(v) The key expansion function takes the key generated from the fingerprint and uses the previously obtained matrix in the RCON function and s_box to develop a key schedule which is 176 bytes long.

(vi) The row-wise arrangement of a circulate matrix can be achieved using the function by calling a sub-function 'cycle'. The cycle performs a right-shift to the previous row of a (4 × 4) matrix.

(vii) The ciphering function takes expanded key, s_box, o, and polymath function from aes_init function and plaintext as input.

Some of the key steps involved are:

- Add round key: It is the XOR between the round key and state matrix.
- Sub-bytes: Performs Exchange using the S_box.
- Shift-rows: All the rows of state matrix is transformed into the left cyclically.
- Mix-columns: The New state matrix is calculated by multiplying the **polynomial** matrix P and the state matrix **S.**

S'=S.

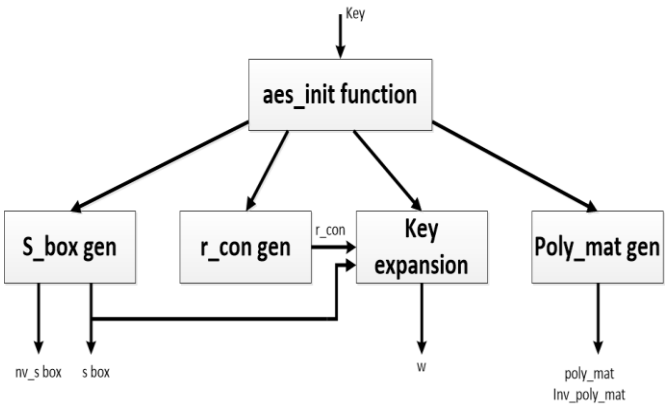

Figure 5. AES_init

4. ENCRYPTION PROCESS

The minutiae are extracted from the fingerprint image. The method used here is as given by Florence Kussener [16].

(i) Enhancement: The fingerprint image obtained from the sensor is enhanced for the minutiae extraction.

(ii) The image is binarized. The ridges are in black and furrows in white.

(iii) Ridges thinning is done to remove the unwanted pixels to make it just one pixel wide.

(iv) A filter is designed to filter a thinned ridged image.

- ✓ If the central pixel is of a value 1 and has only 1 one-valued neighbor, then it is a case of termination.
- ✓ If the central pixel is 1 and has 3 one-value neighbors, then it is a bifurcation.
- ✓ If the central pixel being 1 and has 2 one-value neighbors, it is usual.

(v) The false minutiae have to be processed.

Process 1: if the distance between a bifurcation and a termination has a value lesser than D, then it is eliminated.

Process 2: while the distance between two bifurcations if smaller than D, then it is eliminated.

Process 3: if the distance between two terminations is smaller than D, then it is eliminated.

To determine a region of interest we use binary image and apply to close on this image and an erosion.

(vi) The orientation of different minutiae is obtained

(vii) We save the obtained minutiae terms as (x, y, θ). Only the x term can be used as the specific key for the encryption algorithm. The x terms are obtained in hexadecimal format.

(viii) A six-character password is entered by the patient.

(ix) The password is then transformed into its ASCII equivalent. For obtaining the plain text of length 16-bytes, the user password is flipped and concatenated as follows:

- Let e = [0, 1] where zero is binary 0 and one is binary 1.
- The 16-byte plain text is then obtained as [plaintext, e, flipped plaintext, and e].

(x) The 16-byte key obtained from the fingerprint and the 16-byte password is given to the aes_init function to obtain the cipher.

5. DECRYPTION PROCESS

- ➢ The client provides a fingerprint and a password.
- ➢ The fingerprint is converted to in the specific key and the password is the plain text. These are given in the aes_init function to obtain the cipher.
- ➢ The cipher obtained is matched with that stored in the client database.
- ➢ The match is found the client is verified and the medicine is delivered, else any access is denied.

6. RESULTS

A relational fingerprint database is formed using MySQL. It includes the details of the clients. The various columns in the tables include their name, age, address, and contact number along with the ordered medicine. The fingerprint data of the patients are stored in the ciphered form in the database along with the client-specific password. The AES algorithm used here provides security by generating the key from the fingerprint data of the client and the use of a specific password. On the receiver's side, the fingerprint is taken from the client along with the password, and the cipher is recalculated and matched with the ones present in the database. If the match is found the medicines are delivered.

The system uses the fingerprint data instead of the smart card as used in TMIS systems. This provides security to the data stored in the database as it cannot be retrieved without the user fingerprint as it makes the unauthorized access of the information as it was more likely impossible to superimpose a registered client's fingerprint with impostor fingerprint.

Table 1 shows results obtained for the AES encryption algorithm are shown in the matrix view using MATLAB.

Table 1. Results

Initial State	Initial Round Key
00 00 00 db	ea b9 81 64
00 00 00 0d	06 c6 92 d1
00 00 00 b3	12 95 8a 3e
00 00 b7 69	e9 ea 8e e2
Final State	**Final Round Key**
ea b9 81 64	00 00 00 db
06 c6 92 d1	00 00 00 0d
12 95 8a 3e	00 00 00 b3
e9 ea 8e e2	00 00 b7 69

7. CONCLUSION

The expanded accessibility of lower-cost broadcast communications frameworks and modified patients checking gadgets makes it conceivable to make the benefits of telemedicine straightforwardly into the home of the patient. These telecare medicine information systems allow healthcare delivery services. A protected verification plan will be required to accomplish the objectives of protecting the patient's privacy as well as making sure that he/she gets the correct medical services according to the need. Our research argument thus sums up a better and enhanced way of security features by taking the client's demographic and biometric details and then processing these via certain encryption methods and finally storing them in a relational database. Hence in this way, our proposed algorithm can conclude a secure online based medicine delivery system. A lot of research is to be done in this respect to make the entire system more secure and reliable.

ACKNOWLEDGMENT

We would like to express our special gratitude and thanks to all staff of the Department of Electronics and Communication Engineering, JSSATE Bangalore for their support and cooperation with this work.

REFERENCES

[1] Al-Shibli, A., Al-Jaradi, S. (2017). Electronic pharmacy system (EPS): Case study in Oman. International Journal of Computation and Applied Sciences, 3(3): 284-291.

[2] Kumar, S., Bano, S. (2017). Comparison and analysis of health care delivery systems: Pakistan versus Bangladesh. Journal of Hospital & Medical Management, 3: 1-7. https://doi.org/10.4172/2471-9781.100020

[3] Fung, K.W., Kayaalp, M., Callaghan, F., McDonald, C.J. (2013). Comparison of electronic pharmacy prescription records with manually collected medication histories in an emergency department. Annals of Emergency Medicine, 62(3): 205-211. https://doi.org/10.1016/j.annemergmed.2013.04.014

[4] Yousif, J.H., Alattar, N.N. (2017). Cloud management system based air quality. International Journal of Computation and Applied Sciences, 3(1): 145-152.

[5] Al-Shezawi, M.O., Yousif, J.H., AL-Balushi, I.A. (2017). Automatic attendance registration system based mobile cloud computing. International Journal of Computation and Applied Sciences, 2(3): 116-122. https://doi.org/10.24842/1611/0037

[6] Yousif, J.H. (2015). Classification of mental disorders figures based on soft computing methods. International Journal of Computer Applications, 117(2): 5-11. https://doi.org/10.5120/20524-2857

[7] Yousif, J.H. (2013). Natural language processing based soft computing techniques. International Journal of Computer Applications, 77(8): 43-49. https://doi.org/10.5120/13418-1089

[8] Lamport, L. (1981). Password authentication with insecure communication. Communications of the ACM,. 24(11): 770-772. https://doi.org/10.1145/358790.358797

[9] Sandirigama, M., Shimizu, A., Noda, M.T. (2000). Simple and secure password authentication protocol. IEICE Transactions on Communications, 83(6): 1363-1365.

[10] Haller, N.M. (1994). The s/Key (tm) one-time password system. Symposium on Network and Distributed System Security.

[11] Chen, T.H., Lee, W.B. (2008). A new method for using hash functions to solve remote user authentication. Elsevier Computers & Electrical Engineering, 34(1): 53-62. https://doi.org/10.1016/j.compeleceng.2007.01.001

[12] Mishra, D., Mukhopadhyay, S., Kumari, S., Khan, K.M., Chaturvedi, A. (2014). Security enhancement of a biometric-based authentication scheme for telecare medicine information systems with nonce. Journal of Medical Systems, 38(5): 41. https://doi.org/10.1007/s10916-014-0041-1

[13] Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C., Chung, Y. (2012). A secure authentication scheme for telecare medicine information systems. Journal of Medical Systems, 36(3): 1529-1535. https://doi.org/10.1007/s10916-010-9614-9

[14] Khatoon, S., Rahman, S.M.M., Alrubaian, M., Alamri, A. (2019). Privacy-preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment. IEEE Access, 7: 47962-47971. https://doi.org/10.1109/ACCESS.2019.2909556

[15] Li, X., Wen, Q., Li, W., Zhang, H., Jin, Z. (2014). Secure

privacy-preserving biometric authentication scheme for telecare medicine information systems. Journal of Medical Systems, 38(11): 139. https://doi.org/10.1007/s10916-014-0139-5

[16] Florence, K. Florence Kussener - MATLAB Central. https://www.mathworks.com/matlabcentral/fileexchange/16728-fingerprint-application, accessed on May 13, 2020.

[17] Hao, F., Anderson, R., Daugman, J. (2006). Combining crypto with biometrics effectively. IEEE Transactions on Computers, 55(9): 1081-1088. https://doi.org/10.1109/TC.2006.138

[18] Agarwal, D., Vardhan, A. (2017). AES based symmetric-biometric cryptosystem using user password. Journal of Industrial Pollution Control, 33(2): 1528-1553.

[19] Daemen, J., Rijmen, V. (1998). The block cipher Rijndael. International Conference on Smart Card Research and Advanced Applications, pp. 277-284. Heidelberg. https://doi.org/10.1007/10721064_26