Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 93 (2016) 742 – 750

Procedia Computer Science

6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India

Improved Classical Cipher for Healthcare Applications

Maya Mohan[a],M.K.Kavithadevi[b],Jeevan Prakash V[a,b,*]

[a]*Assistant Professor,Department of CSE,NSSCE,Palakkad-8,India*
[b]*Associate Professor,Department of CSE,TCE,Madurai-15,India*
[a,b,*]*Assistant Professor,Department of Mathematics,NSSCE,Palakkad-8,India*

Abstract

E-health is rapidly picking up the gear and providing lots of services. It facilitates novel solutions for the problems suffered by the aged people as well as the people affected with chronic diseases. Apart from the above services, it devotes much interest in personal fitness. The healthcare system makes use of wearable wireless sensors which are implanted in patients, allow the monitoring of the health status at all time. The data collected from the patients transmitted through the network to the clinic or the doctor for a detailed diagnosis. Since healthcare applications are dealing with highly sensitive data, strong cryptographic algorithms should be incorporated for providing confidentiality. However, due to the computational and energy limitations of wireless devices we are forced to implement light weight ciphers which are computationally feasible in achieving confidentiality. This paper proposes a variant of hill cipher having two key matrices to add extra security to health related data.

Peer-review under responsibility of the Organizing Committee of ICACC 2016

Keywords: Healthcare System; Hill Cipher;WSN;Linear Cryptanalysis;Modular Arithmetic,Matrix Exponentiation

1. Introduction

Health monitoring systems are widely used by all sorts of community worldwide. Lots of research is going in this area to improve the lifestyle of the people [1]. In critical conditions, Wireless Patient monitoring devices [2] which are implanted in patients will help in tracing the internal activities of the patient from time to time. The collected data can

* Corresponding author. Tel.: 919443825095.
E-mail address: mayajeevan@gmail.com

Peer-review under responsibility of the Organizing Committee of ICACC 2016
doi:10.1016/j.procs.2016.07.285

be transferred to healthcare providers or doctors for accelerating the emergency care. A survey [3] conducted in Pakistan reveals the wide acceptability of mobile health systems. The survey highlights the strong demand for healthcare systems. The huge exploitation of healthcare applications necessitates the privacy and security of the user data. In healthcare systems, the main role is played by wireless and mobile devices which are having minimum resources to work. So light weight ciphers, basically with minimum computation are suitable for wireless applications for providing confidentiality [4].In the survey of light weight ciphers, AES implemented in software proved to be more efficient than other light weight ciphers. The proposed Hill cipher is more memory efficient than AES. The proposed algorithm serves as an important pedagogical role in cryptography and algebraic theory. The algorithm guarantees a long way of security from sensors connected with patient till the doctor or the hospital. Hill Cipher [5], [6] was introduced in the year 1929 by Lester S. Hill. It belongs to Polygraphic Cipher [7] which works on a set of letters. Hill Cipher can manage block with varying sizes. Hill cipher works on Linear Algebra, the concept of matrices.. The mathematical nature makes the encryption exact and uncomplicated. Because of the linearity in the operation, Hill cipher undergoes known plaintext attack and not a suitable algorithm for healthcare system. A modified Hill Cipher is proposed [8] by launching two key matrices instead of the one used in Hill Cipher. In this method half the plaintext is encrypted using one key matrix and the next half is encrypted using the second key matrix. EBCDIC code is used in this method. But this is still vulnerable to known plaintext attack. Another modification to Hill Cipher [9], which makes use of one time key matrix for each encryption .The one time key, is calculated by multiplying initial vector which is kept secret to the current key matrix. But it is proven that [10] this is also prone to known plaintext attack. Lots of variants are available for Hill Cipher in the literature with various dimensions of security [11].The proposed scheme could overcome the drawbacks appeared in these papers. The performance analysis of various encryption schemes like RC4, RC5, RC6 and AES are done [12] and the results are compared based on various parameters such as memory usage, computation time, security etc. It is noted that the proposed method showing better efficiency compared to other methods given in the paper. A template has been proposed stating different aspect of cryptography for the secure transfer of knowledge related to healthcare [13]. Various security incidents are analyzed in the paper and proposed solutions for the issues.

Section II of this paper depicts the operation of Hill cipher with more characters up to 37.It highlights the various attacks on Hill cipher. Section III introduces the proposed method illustrated with an example. It highlights the advantages of the proposed system over Hill Cipher. Section IV deals with security concerns of the proposed scheme .Section V gives the implementation results of the proposed scheme.

2. Hill cipher

In order to perform encryption using Hill cipher with modulo 37(character mapping depicted in Table 1), the selected key matrix should be a square matrix of order ' n'. The key matrix should have an inverse with respect to modulo 37. Based on the key matrix the plaintext characters will be selected for encryption. The steps for encryption and decryption are shown below. Assume a Key matrix of order 3,

$$A = \begin{bmatrix} k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 \\ k_7 & k_8 & k_9 \end{bmatrix}.$$

Select a pair of plaintext, consider(p_1, p_2, p_3), the encryption is given in Eq. (1)

$$\begin{bmatrix} k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 \\ k_7 & k_8 & k_9 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} \quad (1)$$

The corresponding decryption operation is given in Eq. (2)

$$\begin{bmatrix} k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 \\ k_7 & k_8 & k_9 \end{bmatrix}^{-1} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \quad (2)$$