RIGHT PATIENT DATA AND OPTIMIZATION PROCESS THROUGH CRYPTOGRAPHIC IMAGE AS KEY USING GENETIC ALGORITHM IN BODY AREA NETWORK

Pradeep Kumar
Ph.D. Student, Enrollment Number: 120481
Mody University of Science and Technology, Lakshmangarh, Sikar-332311, Rajasthan, India

I. INTRODUCTION

Internet of Things (IoT), helping interconnected sensors (i.e., wireless body area network (WBAN), can treat in real time monitoring of patient health status and manage patients and treatment. Likewise, IoT will play a helping role in the next-generation healthcare establishment. Although IoT-based patient health status monitoring has become very popular, monitoring patients remotely outside of hospital settings requires augmenting the capabilities of IoT with other resources for health data storage and processing.

In this paper, we propose an IoT-based authentication and optimization process through image key management using a genetic algorithm in body area network. Recent advances in wireless communications technologies for medical/fitness applications. Particular, it analyzes the following related developments may cover the following topics:

- Status of M2M standardization, market and development in general and specifically for medical/wellness applications
- Development and standardization of the Wireless Body Area Network (WBAN) and Medical Body Area Network (WMBAN), including their markets specifics
- Underlying technologies:
  - Bluetooth and its Medical Profile
  - ZigBee and its Medical Profile
  - Wi-Fi low-power consumption technology
  - Z-Wave, Ant and other technologies
  - Self-powered wireless sensors

II. IMAGE PROCESSING

Mathematically, an image can be considered as a function of 2 variables, f(x, y), where x and y are spatial coordinates and the value of the function at given pair of coordinates (x, y) is called the intensity value.

The programming counterpart of such a function could be a one or two dimensional array. Code Snippet 1 and Code Snippet 2 show how to traverse and use 1-D and 2-D arrays programmatically. Both of them essentially can represent an image as shown in Figure 1.

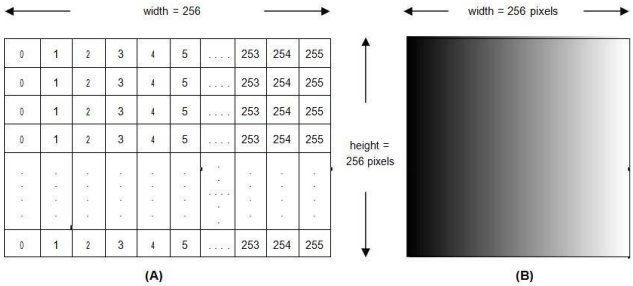

Figure : Values in the grid represent the grayscale intensities of the image on the right.
(A) Intensitiy values shown in a grid of same dimension as image **(B)** Image as seen on monitor

```
A.  Following code declares a 1-D array of type 'unsigned byte' having
B.  size 256*256. It then puts values from 0 through 255 in each row.

int width, height;              // width and height of image
int offset;                     // num of elements traversed in array
int value;                      // image intensity value
width = height = 256;
value = offset = 0;

unsigned byte array_1D[height * width];

for(int j=0; j<height; j++)          //traverse height (or rows)
{
      offset = width * j;            //modify offset travelled
      for(int i=0; i<width; i++)     //traverse width (or columns)
      {
            array 1D[offset + i] = value++;     // update value at
                                                // current index  i.e.
                                                // (offset+i)
      }
      value = 0;
}
```

```
//  Following code declares a 2-D array of type 'unsigned byte' having
//  size 256*256. It then puts values from 0 through 255 in each row.

int width, height;              // width and height of image
int value;                      // image intensity value
width = height = 256;
value = 0;

unsigned byte array 2D[height][width];

for(int j=0; j<height; j++)          // traverse height (or rows)
{
      for(int i=0; i<width; i++)     // traverse width (or columns)
      {
            array 2D[j][i] = value++;      // update value at
                                           // current  (i, j)
      }
      value = 0;
}
```

Code Snippet 2

The 'for' loop in Code Snippet 1 and 2 can be visualized as shown in Figure 2.

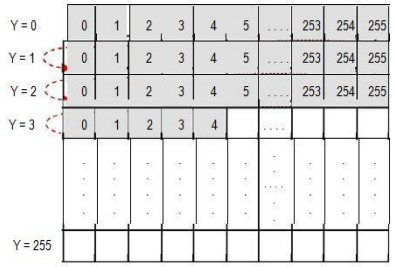

Figure: Array traversal in a 'for' loop. Note that rows are being accessed one after the other. This is known as '*Row Major Traversal*'. The graphic suggests that in the current iteration, x = 4 and y = 3 both starting from 0.

III. SECURITY OPTIMIZATION THROUGH KEY MANAGEMENT USING A GENETIC ALGORITHM IN BODY AREA NETWORK:

A genetic algorithm is a randomized search and optimization technique guided by the principle of natural selection systems. Three basic operators used in Genetic [2] algorithms contain selection, crossover, and mutation. The GA goes through the following cycle: Evaluate, select, mate, and mutate until some stopping criteria are reached. Reproduction and crossover together give genetic algorithms most of their searching power.

Selection It is quantitative criterion based on fitness value to choose the chromosomes from a population which is going to reproduce.

Crossover

In crossover operation, two chromosomes are taken and a new is generated by taking some attributes of the first chromosome and the rest from the second chromosome.[2]

For example, the strings 11001111 to 01101110 could be crossed over after the third locus in each to produce the two offspring 11001110 to 01101111.

Mutation

Mutation is used to maintain genetic diversity from one generation of the population to the next. It is similar to biological mutation. GAs involves string-based modifications to the elements of a candidate solution. These include bit-reversal in bit-string GAs. This operator randomly flips some of the bits in a chromosome. For example, the string 01000100 might be mutated in its second position to yield 00000100.

IV. PROPOSED METHODOLOGY

In the proposed method GA will be used in the key generation process. The crossover and mutation operation is used along with Pseudo-random number generators to make the key very complex. A number of rows in the array can be a population for crossover and mutation purposes. For encryption, we have proposed AES. The symmetric key algorithm is proposed due to its computation speed and less overhead in key management. The process of generating the key from the Genetic Population has the following steps:

STEP 1: A pseudo-random binary sequence is generated with the help of a small image like part of the image of ECG sensor image. Means any image can be used as a cryptographic security key. Another key like sound frequency of patient can be used for a cryptographic key for algorithm or material of a mixture of various metal touches to the sensor can be used for cryptographic security key just like biometric way. As Mathematically, an image can be considered as a function of 2 variables, f(x, y), where x and y are spatial coordinates and the value of the function at given pair of coordinates (x, y) is called the intensity value. The programming counterpart of such a function could be a one or two-dimensional array. The first row of this two-dimensional array can be used as key generated from the same image used for the cryptographic purpose. For more criticality, a random number can be generated to choose the row from the array because the first-row idea can be hacked. But in GA for population limits can be decided for population and for a number of digits through fitness function from rows of the array from image processing.

STEP 2: The generated string or population is divided into two halves.

STEP 3: On the selected string crossover operation is performed to achieve good randomness among the key.

STEP 4: After crossover operation, the bits of the string are swapped again to permute the bit values.

STEP 5: The same process is iterated two times.

Here the crossover and mutation are done two times to create more complexity and randomness in the key. This key will be then used for the encryption process. Here AES will be used for encryption as it is one of the most efficient symmetric key algorithms and its whole security lies in the key used.

V. CONCLUSION

The BAN is an emerging technology that will alter people's everyday experiences revolutionarily. Privacy and data security in BANs is a significant area, and still, there is a number of challenges which need to be overcome. Image processing can create image as a data for cryptographic purposes. So, there is no limit to number of images and so as to number of keys. Mathematical function on keys can help us to more grow in this field.

REFERENCE

[1] Pradeep Kumar, Anand Sharma," Authentication Process In Body Area Network And Security Optimization Through Key Management Using Genetic Algorithm In Body Area Network", ISSN (Online): 2347 – 4718, International Journal For Technological Research In Engineering Volume 4, Issue 9, May-2017,

[2] Aarti Soni, Suyash Agrawal," Using Genetic Algorithm for Symmetric key Generation in Image Encryption", ISSN: 2278 – 1323, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 1, Issue 10, December 2012

[3] Santanu Chatterjee, Ashok Kumar Das *, Jamuna Kanta Sing," A novel and efficient user access control scheme for wireless body area sensor networks", Journal of King Saud University Computer and Information Sciences (2014) 26, 181–201

[4] Copyright © 2005-2007, Advanced Digital Imaging Solutions Laboratory (ADISL). http://www.adislindia.com

