BODY AREA NETWORK TECHNOLOGY AND TO SEND SECURE DATA OF PATIENT THROUGH CRYPTOGRAPHIC KEY ALGORITHM USING IMAGE MATRIX DATA, SOUND MATRIX DATA AND VIDEO URL AS KEY

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

I. ***Abstract:*** ***Wireless body area network can be secured by particle swarm optimization algorithm. 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 artificial intelligence algorithm for security coding for cryptographic key generation taken as recent advances in wireless communications technologies for medical/fitness applications. Security algorithm requires key generation and key can be possible through images matrix through pixel reading and sounds matrix and sound signal coding. If we have many images than body area network is also sensor-based hardware that may require low intensity images for possible software and we can classify required images with the help of particle swarm optimization algorithms to get required key.***

Keywords: Body area network, particle swarm optimization, security keys

---

II. **Image Processing: [1]** An image can be considered as a function of two coordinates like *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 2, show how to traverse and use 1-D and 2-D arrays programmatically. Arrays can be used as key generation through programming actually bits are required for keys generations and we can achieve these bits through image processing programming by creating an array and if it is two-dimensional direct table of bits can be used as key by applying particle swarm optimization for classification and key generation and for safer patient data in using body area network as technology for remote patient treatment. Both of them essentially can represent an image as shown in Figure 1:

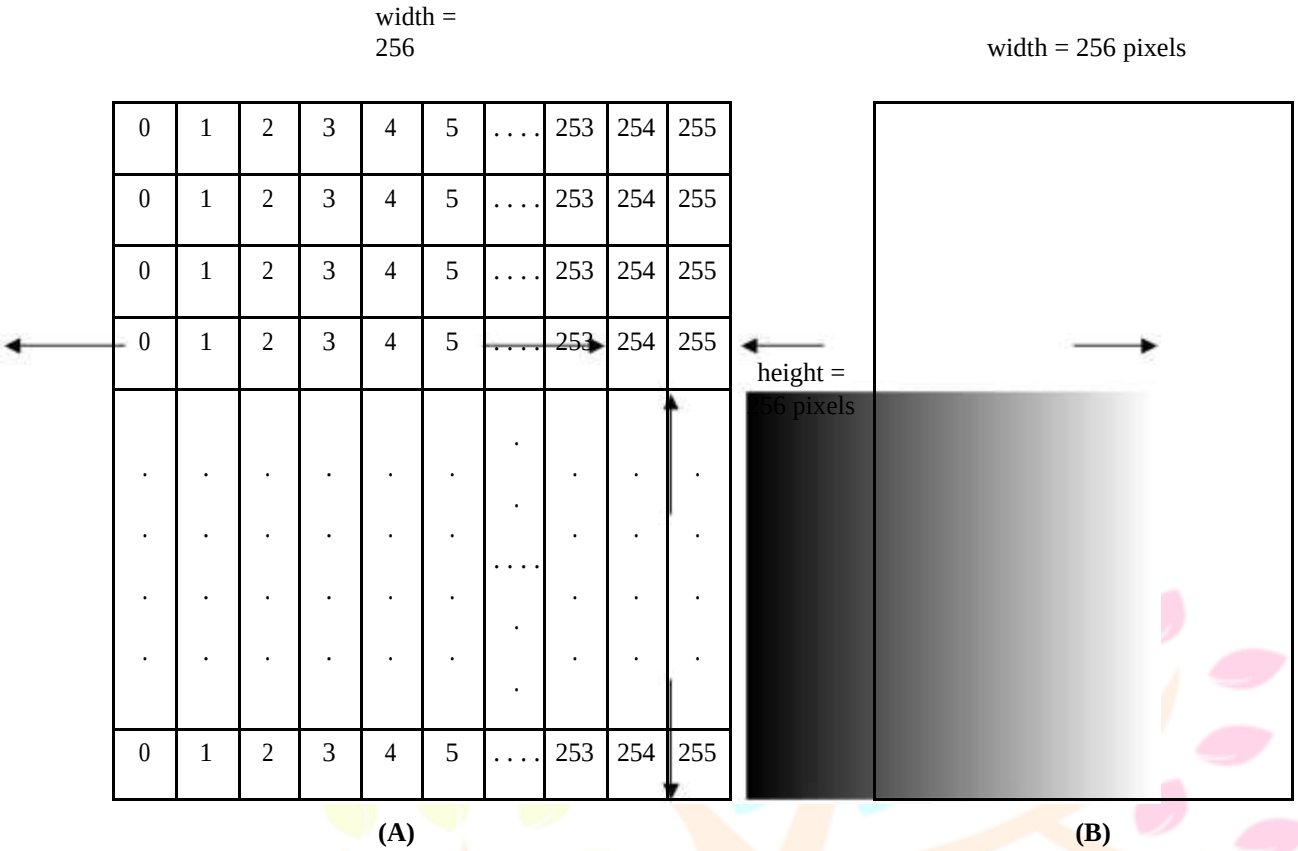

Figure 1: Values in the grid represent the grayscale intensities of the image on the right.

(A) Intensity values are shown in a grid of the same dimension as image **(B)** Image as seen on a 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 traveled
        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.

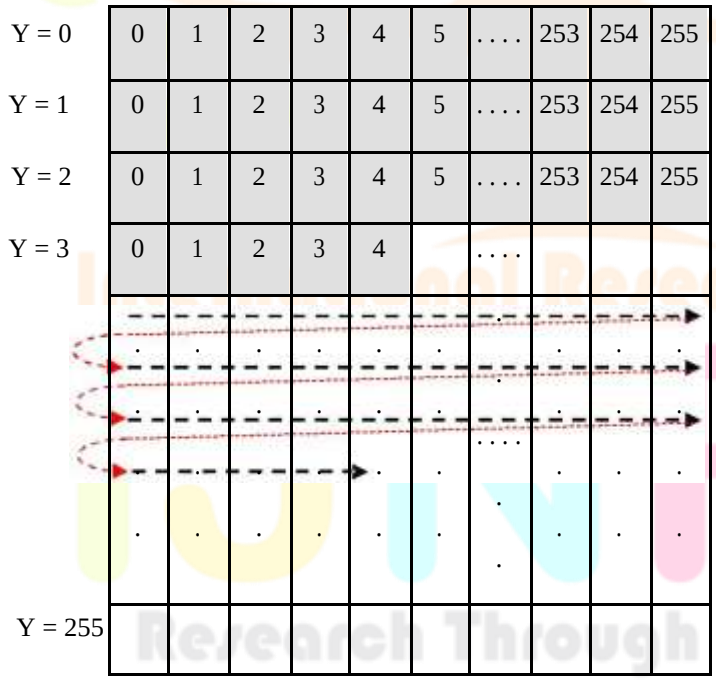

Figure 2: Array traversal in a 'for' loop. Note that rows are being accessed one after the other. This is known as '*Row Major Traversal*'. The graphic suggests that in the current iteration, x = 4 and y = 3 both starting from 0.

Security optimization through key management using a PSO in body area network: Particle Swarm Optimization (PSO) has particle and velocity for judgement as symbolic parameters for reaching to low intensity images from large sets of images. It is based on swarm intelligence. PSO optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measure of quality and security key can be generated by this iteration and possible randomization. Before performing the actual classification, an aggregation process is needed to reduce the amount of extra data which got generated while trying security keys from various images. Aggregated data is stored to a DataMart, and the data in the DataMart is divided into a raw data set and test data set. The raw data set is use for making rules and the test data set is used for evaluating the accuracy of the rules.

III. PROPOSED METHODOLOGY

In the proposed method Swarm particle optimization algorithm can be used as classification and used in the key generation process. 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 Particle swarm optimization has the following steps:

STEP 1: From various images of various intensities and from various sound signal we can classify images and sound signals which are suitable for key size in body area network which require low powered arrangements. Images with low intensities can be separated through classification and be given for next step for cryptographic purpose.

STEP 2: A binary sequence is generated with the help of a small image like part of the image of ECG sensor image through the image processing computer programming. Means any image can be used as a cryptographic security key through reading functions for matrix. Similarly, image generated from metal touch made up of mixture of various material can be used for cryptographic security key just like biometric way. Any number of such mixture of metal can be created and its touch to sensor can create different images means any number of keys through image processing computer programming and similar mixture of metal can be kept at both ends.

STEP 3. In computer program, 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. More criticality, a random number can be generated to choose the row from the array because the first-row idea can be hacked.

STEP 4. Through computer coding in particle swarm optimization, limits of allowed number of digits for key can be decided for better speedy results with the fitness function from generated rows of the array in computer program from the concept image processing. Fitness function like converting first row of two-dimensional array carrying bits into a decimal number and the new decimal number generated by this process can be divided by hundred or more as per optimality factor after experimentation to reduce the bit size to convert this number back into binary and can be used as the population of cryptographic reduced key in lesser number of digits as per hardware availability and requirement.

STEP 5. For highly insecure environment coding can be changed to use of two images by intermixing of arrays to increase the population to create double lock environment

STEP 6. Matrix from sound programming computation can be used as key if the image is not available.

STEP 7. For internet environment video URL can be used for generating key that can be generated similarly as reference [4]. For distributed environment in this way we can generate many number of keys and can send different keys to different users in networks to access the secure data. Means as many number of clients we can generate that many keys for more authentications.

STEP 8: Other option is to take two sound signals for two keys generation as double lock for security in transfer of data in body area network

STEP 9: Particle Swarm Optimization Classification Algorithm can take result as:

Input: raw data as image matrix or/and sound matrix
repetition number (generate initial particles (=threshold rule) randomly)
for repetition number do {for each particle do {
Calculate the fitness value as low intensity image using raw data for
finding the pbest; end for;
find the gbest;
for each particle do {compute velocity and update particle; end for}
end for}
output: rule same as gbest, we can choose gbest as key.

IV. CONCLUSION

Privacy and data security in body area networks is a significant area, and still, there is a number of challenges which need to be overcome. Image processing can create an image as a data for cryptographic purposes. So, there is no limit to a number of images and so as to the number of keys. Mathematical function on keys can help us to more growth in this field. Particle swarm optimization can be used for classification among images, which can be used for security key in body area networks. Distributed environments can be used as body area network as different security keys for different clients. As internet speed is entering 5G than multimedia use for security key will be speed justified. App culture and allowed sensor possible attachments with smart phones can easily allow transfer of sensor data and app coding can use this security key arrangement. Government may adopt this every hand arrangement of remote patient data monitoring system development.

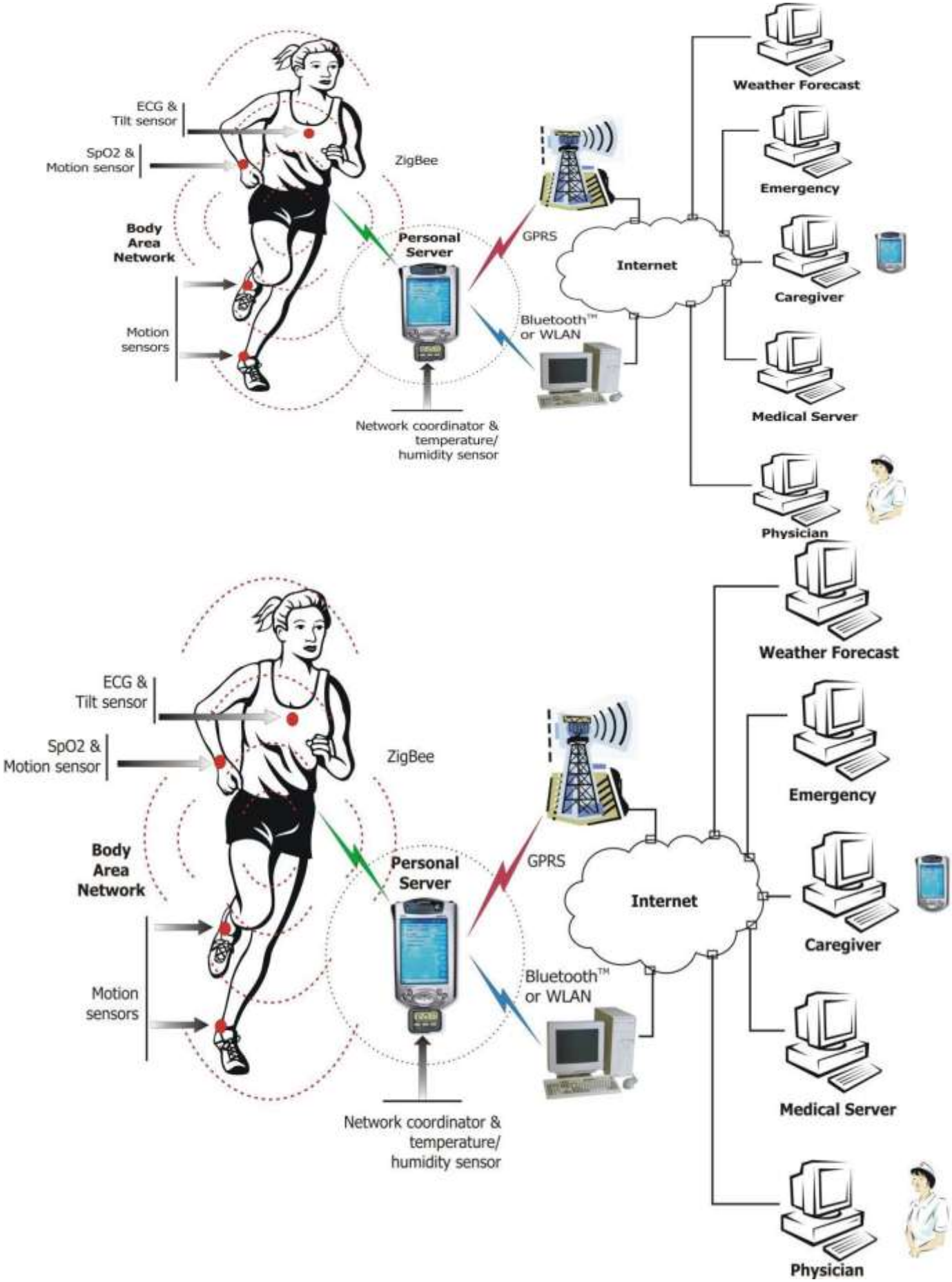

Figure 3. sensors with smart phone

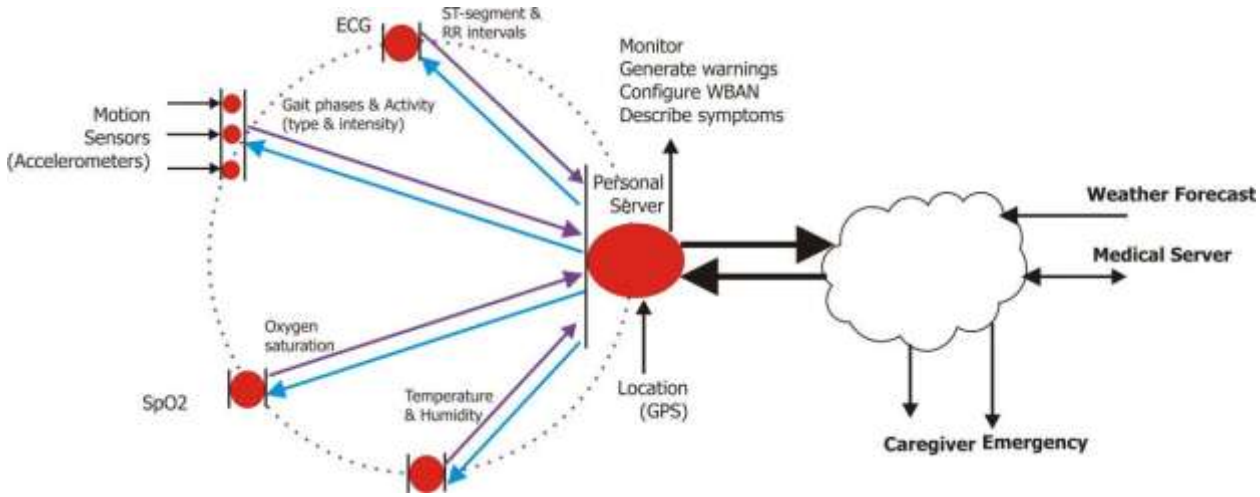

Figure 4. Data flow diagram of sensors with smart phone

V. References:

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

[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] Pradeep Kumar," Right Patient Data and Optimization Process Through Cryptographic Image as Key Using Genetic Algorithm in Body Area Network", ISSN (Online): 2347 – 4718, International Journal for Technological Research In Engineering Volume 5, Issue 9, May- 2018

[4] Prajakta Jadhav1 Sonal Sangale2 Rajeshwari Variar3 Prof. Madhuri Ghuge4 1,2,3Student 4 Assistant Professor 1,2,3,4," Video Encryption & Decryption Using Parallel AES Algorithm" Department of Computer Engineering 1,2,3,4Bharati Vidyapeeth College of Engineering, Navi Mumbai-400614, IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 10, 2014 | ISSN (online): 2321-0613

[5] Pooja Mohnani, PhD Scholar at Jain University, Assistant Professor, Jayalakshmi H.M Mtech student CMRIT,"Particle Swarm Optimization used for classification of ECG & Blood sugar data in WBAN environment"