Android base Healthcare Monitoring and Management System using IoT

Akshay Chavan[1], Pratiksha Deshmukh[2], Vallabh Patil[3], D. S. Hirolikar[4]

[1,2,3]Student, Information Technologies of PDEA's College 0f Engineering, Manjari(Bk), Pune, Maharashtra, India
[4]Professor, Information Technologies of PDEA's College 0f Engineering, Manjari(Bk), Pune, Maharashtra, India

---

Abstract - Advances in data and communication technology have caused the emergence of web of things (IoT). within the present day healthcare surroundings using IoT technologies brings comfort of physicians and sufferers considering that they're applied to various scientific regions (which include actual-time tracking affected person facts management and healthcare management). The body sensor network (BSN) generation is one in all the middle technology of IoT traits in health-care gadget, during which a affected person could also be monitored the usage of a group of tiny-powered and light-weight WI-FI sensor nodes. But, development of this new era in healthcare programs without thinking concerning protection makes patient privacy in Health-Care. initially we tend to highlight the most protection necessities in BSN primarily based all current healthcare machine. Further, we tend to propose a secure IoT primarily based all health-care contrivance the utilization of BSN, known as BSN-Care, that may with efficiency accomplish those wants.

Key words: BSN- BODY Sensor Network, Data integrity, Authentication, e-Health, Internet-of-Things, Security and reliability issues in distributed applications.

1. INTRODUCTION

Recently, the explanation for a patient staying within the hospital isn't that he or she really wants active treatment. Often, the principal reason for a long keep within the hospital is solely continual observation. Therefore, efforts are created to avoid acute admissions and long lengths of keep within the hospital. Wireless sensing element Networks (WSNs) with intelligent sensor nodes are getting important sanctionative technology for big selection applications. Recent technological advances in integrated digital physical science and shrinking of physical sensors, microchip, and oftenness devices into one micro-chip has junction rectifier to the emergence of terribly light-weight, ultra-low power, observance sensing element devices. These sensing element devices have the aptitude of sensing, process and transmittal very important physiological signals exploitation wireless technology.

Contrary to the quality device networks that are rigorously planned and deployed within the preset positions, WSNs are often deployed in associate ad-hoc manner that build them strong, fault tolerance, and increase in abstraction coverage. they'll greatly be wont to monitor and track conditions of patients in each cities and rural areas victimization an computer network or net thereby reducing the strain and strain of attention suppliers, eliminate medical errors, scale back work, increase potency of hospital workers, scale back long price of attention services, and improve the comfort of the patients. Also, these systems give helpful strategies to remotely acquire and monitor the physiological signals while not the necessity of interruption of the patient's traditional life, so up life quality. device nodes are often strategically placed on the soma to make a cluster that's referred to as wireless body space network (WBAN) which will be wont to collect patient's very important signs. it's value noting that device nodes are being operated by batteries, their power consumption throughout transmission should be stripped-down for economical and reliable information transmission between WBAN and private server.

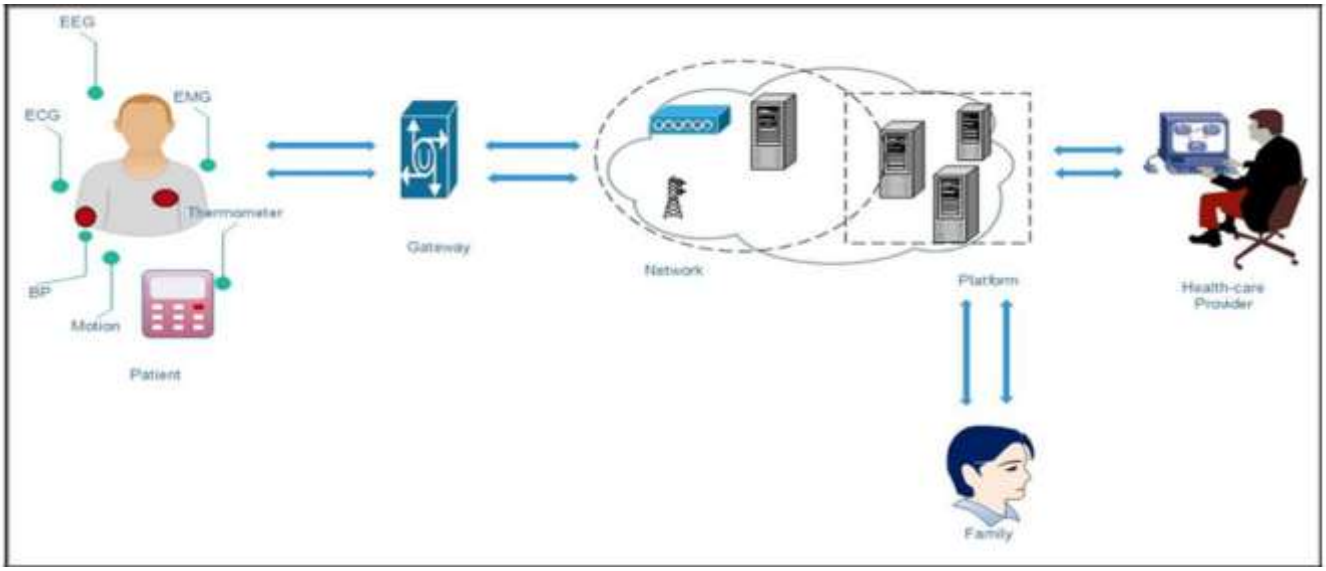
2. SYSTEM DESCRIPTION

2.1 Functionality summary

The core of this system is the user called the patient. Wearable sensors are attached to the patient body forming wireless body sensor network (BSN)[5] to monitor changes in patients vital signs closely and provide real time feedback to help maintain an optimal health status. The medical sensors typically consist of five main components:

1) Sensor (2) Microcontroller (3) Memory (4) Bluetooth Transceiver (5) Power supply.

1) Sensor: Read Patient vital signs closely.
2) Microcontroller: Compute Sensor values.
3) Memory: Manage and log the data
4) Bluetooth Transceivers: To communicate with server
5) Power supply: To supply the power



Flow of System:

a) Different sensors are attached to the patient body like ECG, Thermometer, Pulse sensor, etc.
b) That sensor sense the patient body condition and sends that values to the Health Care Centre vie BSN.
c) Health Care Centre get that values and generate reports based on that values and analyse that values & gives the valuable response or feedback to the patient as below:

   I. If patient condition were critical then health care centre involves patient family by sending alert message to them. And health care centre also sends the patient details and location of patient to nearest hospital with its reports.
   II. If patient condition were normal then health care centre sends or provides the some valuable tips to patient.

3. LITERATURE SURVEY

1) "BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network"- Prosanta Gope, Tzonelih Hwang* 2015.2502401 IEEE Sensors Journal.[1]

In this article, at first we highlight the major security requirements in BSN based modern healthcare system. Subsequently, they propose a secure IoT based healthcare system using BSN, called BSN-Care, which can efficiently accomplish those requirements

2) "Towards Realizing a Self-Protecting Healthcare Information System."-Qian Chen and Jonathan Lambright - 2016 IEEE 40th Annual Computer Software and Applications Conference.[2]:

In this paper they discuss the present security challenges of HISs, and styles AN involuntary Security Management (ASM) approach, that proactively self-protects a HIS from internal and external attacks? The performance of a HIS is monitored in real time, and potential attacks which will disrupt HIS services are expected by the intrusion estimation module. They conjointly discuss the practicality and practicability of intrusion detection systems for police work legendary and unknown cyber-attacks threatening then confidentiality and integrity of EHRs. The intrusion response system of the ASM approach selects the foremost acceptable protection mechanisms to recover the compromised HIS back to traditional with very little or no human intervention.

3) A "A Mobile Health Monitoring Application for Obesity Management and Control Using the Intemet-of-Things",Mohamed Alloghani Abir Hussain!, Dhiya AI-Jumeily! Paul Fergus!, Omar Abuelma'atti, Hani Hamden.[3]:

This paper presents a mobile health application meant to extend the attention levels of oldsters and kids concerning the blubber risks and facilitate them to sustain balanced and healthy intake life-style. The projected mobile application is an academic tool for the analysis of interventions to stop blubber risk levels. the applying relies on the net of Things approach, that permits trailing food intake, remote capturing and constant observation of youngsters knowledge with interactive feedback displayed on the mobile application.

4) "Exploiting the FIWARE Cloud Platform to Develop a Remote Patient Monitoring System" - Maria Fazio , Antonio:

This System aims to allow care givers to improve remote assistance to patients at home, optimizing the management of the workflow of doctors, physicians, medical assistants, and other involved hospital operators. In this paper, they specifically describe the main FIWARE components that they had adopted to design their architecture and how they have been integrated.

5) "A Health Care Self-Monitoring System for Patientswith Visual Impair-ment using a Network of Sensors",Oana GEMAN1, Iuliana CHIUCHISAN-The,5th IEEE International Conference on E-Health .[5]

They intend to improve their quality of life by creating a low-cost health care self-monitoring system using a network of sensors that transmits the biomedical information played by voice to the patient and help him to move and to know the exact location of obstacles, using a sound signal received in headphones or speakers.

4. ALGORITHM

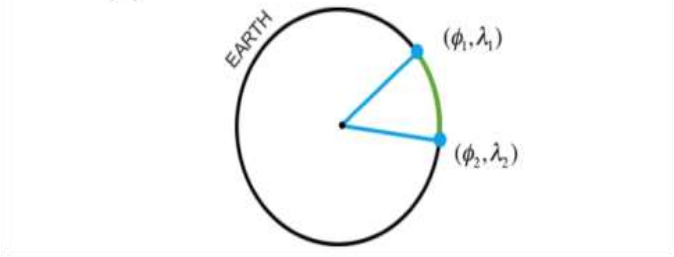
1) The Haversine's

Haversine's pseudo code for determining the great-circle distance between two points on a sphere given their longitudes and latitudes.

Location_Nearest = a cos (sin (lat1*PI ()=180) * sin (lat2 * PI ()=180)+(cos(lat1 * PI ()=180)* cos (lat2 * PI ()=180) * cos(lon2 * PI ()=180 - lon1 * PI () =180))) * 3956

For any two points on a sphere, the haversine of the central angle between them is given by,

$$\text{haversine}\left(\frac{d}{r}\right) = \text{haversine}(\phi_2 - \phi_1) + \cos(\phi_1)\cos(\phi_2)\text{haversine}(\lambda_2 - \lambda_1)$$



Where,

- hav is the haversine function.

$$hav(\Theta) = sin^2\left(\frac{\Theta}{2}\right) = \frac{1-cos(\Theta)}{2}$$

- d is the distance between the two points (along a great circle of the sphere; see spherical distance),
- r is the radius of the sphere,
- 1 , 2: latitude of point 1 and latitude of point 2, in radians
- 1, 2: longitude of point 1 and longitude of point 2, in radians

2) The MD5 Message-Digest Algorithm

Step 1. Append cushioning Bits

The message is "padded" (extended) in order that its length (in bits) is congruent to 448, modulo 512. That is, the message is extended in order that it's simply sixty four bits keep of being a multiple of 512 bits long. Cushioning is usually performed, albeit the length of the message is already congruent to 448, modulo 512.

Padding is performed as follows: one "1" bit is appended to the message, then "0" bits square measure appended in order that the length in bits of the soft message becomes congruent to 448, modulo 512. In all, a minimum of one bit and at the most 512 bits square measure appended.

Step 2. Append Length

A 64-bit illustration of b (the length of the message before the cushioning bits were added) is appended to the results of the previous step. Within the unlikely event that b is bigger than 2^64, then solely the low-order sixty four bits of b square measure used. (These bits square measure appended as 2 32-bit words and appended low-order word initial in accordance with the Previous conventions.)

At now the ensuing message (after cushioning with bits and with b) contains a length that's a particular multiple of 512 bits. Equivalently, this message contains a length that's a particular multiple of sixteen (32-bit) words. Let M[0 ... N-1] denote the words of the ensuing message, wherever N could be a multiple of sixteen.

Step 3. Initialize MD Buffer

A four-word buffer (A,B,C,D) is employed to reckon the message digest. Here every of A, B, C, D could be a 32-bit register. These registers square measure initialized to the subsequent values in hex, low-order bytes first):

word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10

Step 4. Process Message in 16-Word Block

We first define four auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word.

F(X,Y,Z) = XY v not(X) Z
G(X,Y,Z) = XZ v Y not(Z)
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X v not(Z))

In each bit position F acts as a conditional: if X then Y else Z. The function F could have been defined using + instead of v since XY and not(X)Z will never have 1's in the same bit position.) It is interesting to note that if the bits of X, Y, and Z are independent and unbiased, the each bit of F(X,Y,Z) will be independent and unbiased.

The functions G, H, and I are similar to the function F, in that they act in "bitwise parallel" to produce their output from the bits of X, Y, and Z, in such a manner that if the corresponding bits of X, Y, and Z are independent and unbiased, then each bit of G(X,Y,Z), H(X,Y,Z), and I(X,Y,Z) will be independent and unbiased. Note that the function H is the bit-wise "xor" or "parity" function of its inputs.

This step uses a 64-element table T[1 ... 64] constructed from the sine function. Let T[i] denote the i-th element of the table, which is equal to the integer part of 4294967296 times abs(sin(i)), where i is in radians.

```
Do the following:

/* Process each 16-word block. */
     For i = 0 to N/16-1 do

/* Copy block i into X. */
       For j = 0 to 15 do
       Set X[j] to M[i*16+j].
       end /* of loop on j */

/* Save A as AA, B as BB, C as CC, and D as DD. */
       AA = A
       BB = B
       CC = C
       DD = D

 /* Round 1. */
       /* Let [abcd k s i] denote the operation
       a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s). */
       /* Do the following 16 operations. */
       [ABCD 0 7 1] [DABC 1 12 2] [CDAB 2 17 3] [BCDA 3 22 4]
       [ABCD 4 7 5] [DABC 5 12 6] [CDAB 6 17 7] [BCDA 7 22 8]
       [ABCD 8 7 9] [DABC 9 12 10] [CDAB 10 17 11] [BCDA 11 22 12]
       [ABCD 12 7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA 15 22 16

 /* Round 2. */
       /* Let [abcd k s i] denote the operation
       a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s). */
       /* Do the following 16 operations. */
       [ABCD 1 5 17] [DABC 6 9 18] [CDAB 11 14 19] [BCDA 0 20 20]
       [ABCD 5 5 21] [DABC 10 9 22] [CDAB 15 14 23] [BCDA 4 20 24]
       [ABCD 9 5 25] [DABC 14 9 26] [CDAB 3 14 27] [BCDA 8 20 28]
       [ABCD 13 5 29] [DABC 2 9 30] [CDAB 7 14 31] [BCDA 12 20 32]

 /* Round 3. */
       /* Let [abcd k s t] denote the operation
       a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s). */
       /* Do the following 16 operations. */
       [ABCD 5 4 33] [DABC 8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]
       [ABCD 1 4 37] [DABC 4 11 38] [CDAB 7 16 39] [BCDA 10 23 40]
       [ABCD 13 4 41] [DABC 0 11 42] [CDAB 3 16 43] [BCDA 6 23 44]
       [ABCD 9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA 2 23 48]

/* Round 4. */
       /* Let [abcd k s t] denote the operation
       a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s). */
       /* Do the following 16 operations. */
       [ABCD 0 6 49] [DABC 7 10 50] [CDAB 14 15 51] [BCDA 5 21 52]
       [ABCD 12 6 53] [DABC 3 10 54] [CDAB 10 15 55] [BCDA 1 21 56]
       [ABCD 8 6 57] [DABC 15 10 58] [CDAB 6 15 59] [BCDA 13 21 60]
       [ABCD 4 6 61] [DABC 11 10 62] [CDAB 2 15 63] [BCDA 9 21 64]

/* Then perform the following additions. (That is increment each
       of the four registers by the value it had before this block
       was started.) */
       A = A + AA
       B = B + BB
       C = C + CC
       D = D + DD

end /* of loop on i */
```

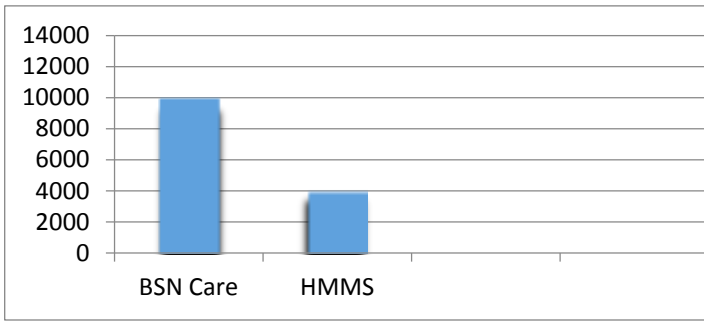
Step 5. Output

The message digest produced as output is A, B, C, D. That is, we begin with the low-order byte of A, and end with the high-order byte of D.

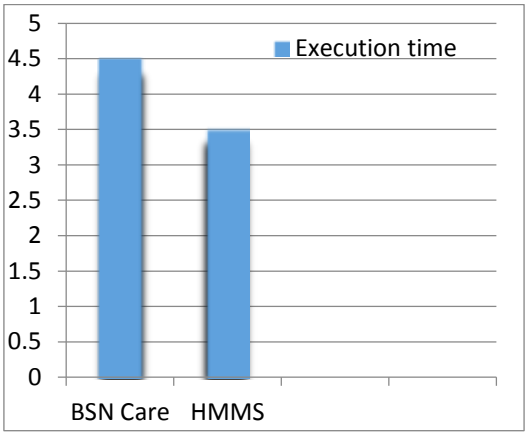
5. ANALYSIS

Analysis of system:

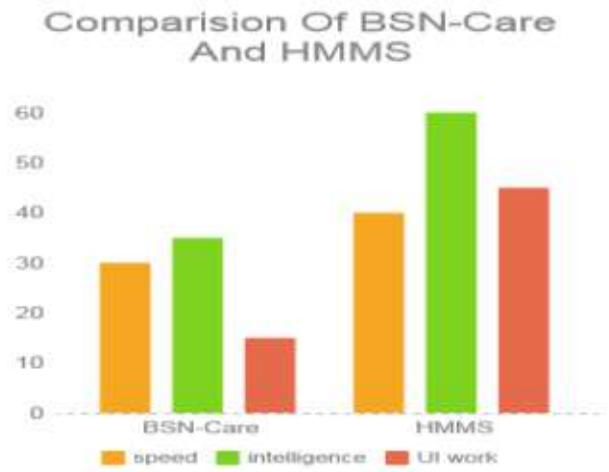
The motivation behind the proposed plan is to determine a few security issues existing in BSN based human services framework and furthermore to ensure sensible computational overhead. In this segment, we look at our proposed HMMS Care human services framework with the best in class BSN based medicinal services frameworks, to show the upsides of the proposed conspire. Presently, despite the fact that all the current state of the workmanship HMMS based social insurance arrangements, what's more, [10] tended to the necessity for security and protection for the touchy information, yet just two of them i.e Alarm-net[8] and Median [9] implanted any security. In this manner, in request to break down the execution of the proposed plot particularly on the security front, our proposed plot has been contrasted and [8] and [10] as far as the different security necessities of the HMM System. Plainly the proposed HMM System can fulfill all the security necessities of the BSN based human services framework. Conversely, even in spite of the fact that both the AES-CBC encryption and CBC-MAC, utilized as a part of BSN-care consider the necessity of a protected verification conspire, however which validation convention they have utilized still obscure. Furthermore, none of them and has considered the properties like secrecy, secure restriction, and so forth which are incredibly vital. To the best of our insight, this is the principal lightweight unknown validation convention for IoT based medicinal services framework that can ensure all the basic components (e.g. shared confirmation, solid client protection safeguarding, secure confinement) of system security.



Graph: Performance Benchmarking based on CPU Cycles



Graph: Performance Benchmarking based on Execution Time



Graph: Comparison of BSN-care and HMM System

Analysis on algorithm:

1. A fourth round has been added.
2. Each step now has a unique additive constant.
3. The function g in round 2 was changed from (XY v XZ v YZ) to (XZ v Y not(Z)) to make g less symmetric.
4. Each step now adds in the result of the previous step. This promotes a faster "avalanche effect".
5. The order in which input words are accessed in rounds 2 and 3 is changed, to make these patterns less like each other.
6. The shift amounts in each round have been approximately optimized, to yield a faster "avalanche effect." The shifts in different rounds are distinct.

Below table shows difference between SHA and MD5 algorithm

Keys For Comparison	MD5	SHA
Security	Less Secure than SHA	High Secure than MD5
Message Digest Length	128 Bits	160 Bits
Attacks required to find out original Message	2^{128} bit operations required to break	2^{160} bit operations required to break
Attacks to try and find two messages producing the same MD	2^{64} bit operations required to break	2^{80} bit operations required to break
Speed	Faster, only 64 iterations	Slower than MD5, Required 80 iterations
Successful attacks so far	Attacks reported to some extents	No such attach report yet

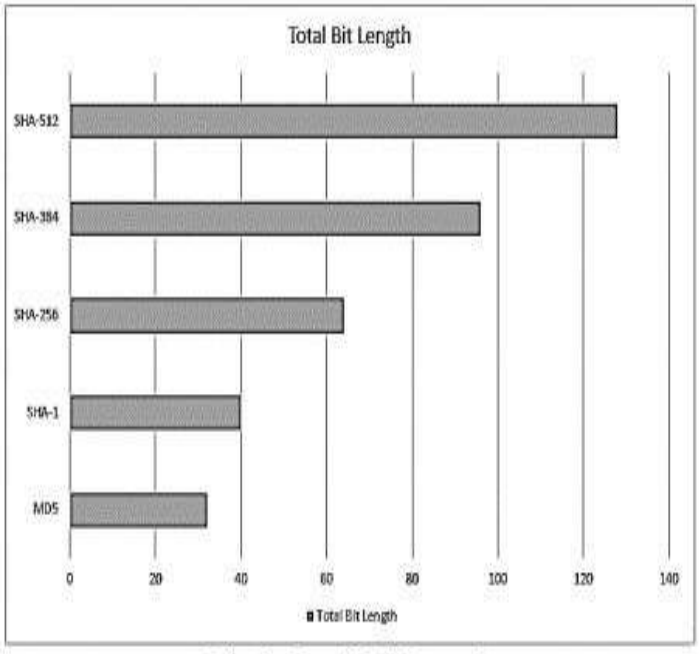


Fig 3: Total Bit Length

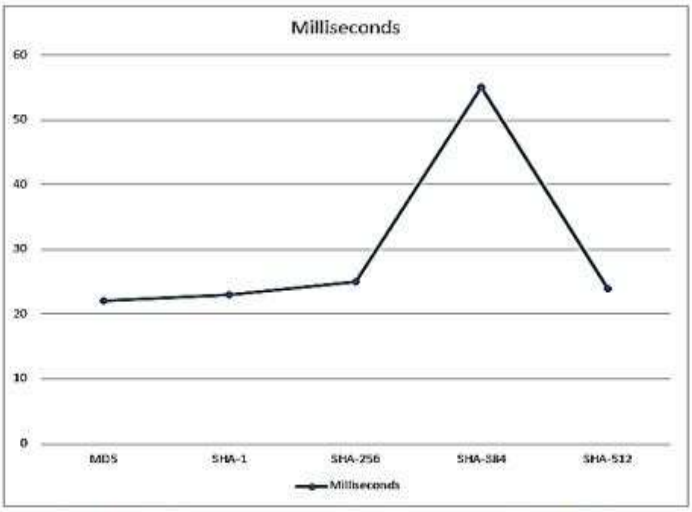


Fig 4: Performance chart of hashing algorithms

6. CONCLUSION

We reviewed this state and projected future directions for integration of remote health observation technologies into the clinical apply of medication. Wear-able sensors, significantly those equipped with IoT intelligence, supply enticing choices for sanctionative observation and recording of knowledge in home and work environments, over for much longer durations than are presently done at workplace and laboratory visits. This treasure hoarded wealth of knowledge, once analyzed and bestowed to physicians in easy-to-assimilate visualizations has the potential for radically up tending and reducing prices. we have a tendency to highlighted many of the challenges in sensing, analytics, and mental image that require to be addressed before systems may be designed for seamless integration into clinical apply.

REFERENCES

[1] "BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network"-Prosanta Gope, Tzonelih Hwang* 2015.2502401 IEEE Sensors Journal.

[2] "Towards Realizing a Self-Protecting Healthcare Information System" Qian Chen and Jonathan Lambright -2016 IEEE 40th Annual Computer Software and Applications Conference Open Data Copenhagen: http://data.kk.dk/

[3] Spira, "A Mobile Health Monitoring Application for Obesity Management and Control Using the Intemet-of-Things",Mohamed Alloghani Abir Hussain!, Dhiya AI-Jumeily!, Paul Fergus!, Omar Abuelma'atti, Hani Hamden

[4] "Exploiting the FIWARE Cloud Platform to Develop a Remote Patient Monitoring System" Maria Fazio,Antonio Celesti , Fermn Galan Marquez, Alex Glikson, Massimo Villari.

[5] "A Health Care Self-Monitoring System for Patients with Visual Impairment using a Network of Sensors",Oana GEMAN1, Iuliana HIUCHISAN The,5th IEEE International Conference on E-Health

[6] "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing: Opportunities and Challenges." Moeen Hassanalieragh, Alex Page, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo MateosBurak Kantarci, Silvana Andreescu.

[7] "Internet of Things: Remote Patient Monitoring Using Web Services and Cloud Computing" - 2014 IEEE International Conference on Internet of Things (iThings 2014), Green Computing and Communications (GreenCom 2014), and Cyber-Physical-Social Computing (CPSCom 2014)

[8] "Survey Based Analysis of Internet of Things Based Architectural Framework for Hospital Management System."-Amna Pir, M. Usman Akram, Muazzam A. Khan., 2015 13th International Conference on Frontiers of Information Technology

[9] Byung-In S. Pai, M. Meingast, T. Roosta, S. Bermudez, S. Wicker, D. K. Mulligan , S. Sastry, "Condentiality in Sensor Networks: Transactional Information," IEEE Security and Privacy Magazine. 2008.

[10] J.W.P. Ng, B.P.L Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, G. Yang, "Ubiquitous Monitoring Environment for Wearable and Implantable Sensors(UbiMon)," Proceedings of 6th International Conference on Ubiquitous Computing (UbiComp04); Nottingham, UK. 714 September 2004.

[11] Ofce for Civil Rights, United State Department of Health and Human Services Medical Privacy. National Standards of Pro-tect the Privacy of Personal-Health-Information. Available online: http://www.hhs.gov/ocr/privacy/hipaa/administra tive/pri vacyrule/inde x.html (accessed on 15 June 2011).

[12] R. Chakravorty, "A Programmable Service Architecture for Mobile Medical Care," Proceedings of 4th Annual IEEE International Conference on Pervasive Computing and Communication Workshop (PERSOMW06); Pisa, Italy. 1317 March 2006.

[13] J. Ko, J. H. Lim, Y. Chen, R. Musaloiu-E, A. Terzis, G. M. Masson, "Me-dian: Medical Emergency Detection in Sensor Networks," ACM Trans. Embed. Comput. Syst. vol. 10, pp. 129, 2010.