ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 3, Issue 3, March 2014*

# Cloud-Assisted Privacy Preserving Mobile Health Monitoring Using PPSPC technique

**M.B.Sushrutha**

Student- M.Tech, Department of Computer Science & Engineering, Cambridge Institute of Technology, Bangalore, India

**Abstract**: Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology. In this paper we discuss about attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique, and allows a medical user to decide who can participate in the opportunistic computing to ensure privacy.

**Keywords**: CAM, Mobile-Healthcare emergency, opportunistic computing, user-centric privacy access control, PPSPC

## I. INTRODUCTION

Wide deployment of mobile devices, such as smart phones equipped with low cost sensors, has already shown great potential in improving the quality of healthcare services. Remote mobile health monitoring has already been recognized as not only a potential, but also a successful example of mobile health (mHealth) applications especially for developing countries. The Microsoft launched project "MediNet" is designed to realize remote monitoring on the health status of diabetes and cardiovascular diseases in remote areas in Caribbean countries. In such a remote mHealth monitoring system, a client could deploy portable sensors in wireless body sensor networks to collect various physiological data, such as blood pressure (BP), breathing rate (BR), Electrocardiogram (ECG/EKG), peripheral oxygen saturation (SpO2) and blood glucose. Such physiological data could then be sent to a central server, which could then run various web medical applications on these data to return timely advice to the client.

### A. *The main contributions of this paper are:*

1. User-centric privacy access control in opportunistic computing, we present an efficient attribute based access control and a novel non-homomorphic encryption based privacy preserving scalar product computation (PPSPC) protocol.
2. The effectiveness of this framework in m-Healthcare emergency, we also develop a custom simulator built in Java. Extensive simulation results show that the proposed framework can help medical users.

## II. EXISTING SYSTEM

In the Existing system, with the pervasiveness of smart phones, mobile Healthcare (m-Healthcare), which extends the operation of Healthcare provider into a pervasive environment for better health monitoring, has attracted considerable interest recently. However, the flourish of m-Healthcare still faces many challenges including information security and privacy preservation.

### A. *Limitations*

1. The flourish of m-Healthcare still faces many challenges including information security and privacy preservation.
2. The Smartphone's energy could be insufficient when an emergency takes place.

## III. PROPOSED SYSTEM

In this paper, we propose a new secure and privacy-preserving opportunistic computing framework, called CAM, to address this challenge. With the proposed CAM framework, each medical user in emergency can achieve the user-centric privacy access control to allow only those qualified helpers to participate in the opportunistic computing to balance the high reliability of process and minimizing privacy disclosure in m-Healthcare emergency. We introduce an efficient user-centric privacy access control in CAM framework, which is based on an attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique, and allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming data.

### A. *System model*

In health care responsible health care benefits of our system, a medical personnel at the centre who is considered trustworthy is for initializing and controlling the entire system. A user who wishes to get the mobile healthcare system registers himself as a medical user under a particular health care centre, then a medical professional examines the user and generates his health profile. Based on the health profile, the users are then provided with the particular type of data such as heart rate, blood sugar level and other materials. Once being equipped with the sensors the users can move anywhere unlike in hospital.[1] The sensors begin to collect the sensed data and transmit them to the user's smart phone which is then transmitted to the health care center. The s the smart phone plays a vital role in mobile monitoring of patients. The smart phones are used for various purposes, the power of the smart phone may not be sufficient under emergency circumstances. Hence we make use of opportunistic computing where whenever a medical user is in emergency other medical users in the nearby area can contribute their resources.

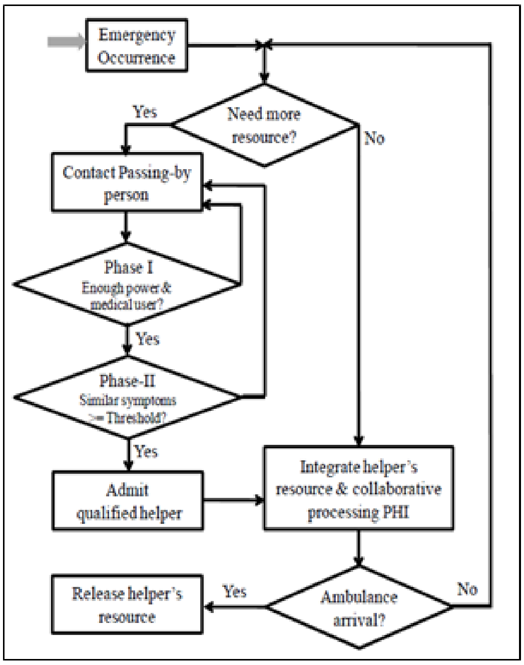

Emergency Occurrence
Need more resource?
Yes
No
Contact Passing-by person
Phase I
Enough power & medical user?
Yes
Phase-II
Similar symptoms >= Threshold?
Yes
Admit qualified helper
Integrate helper's resource & collaborative processing PHI
Release helper's resource
Yes
Ambulance arrival?
No

Fig. 1 Opportunistic computing with two-phase privacy access control for m-Healthcare emergency

### A. PPSPC Framework

In this section, we propose our PPSPC framework which focuses on initializing the system, the scenario depicting healthcare care monitoring under normal conditions and the health care monitoring during emergency situations.

### B. Initializing the system

According to our work, the person at the health care centre is responsible for initializing the entire system. The authority at the health care center generates the bilinear parameters () by running gen(sp) using the security parameter (sp).He also selects the encryption algorithm that is to be used, two secure cryptographic hash functions H and H´, two random elements (h1,h2) in G1 is choosen also the master key is selected by choosing two random numbers (a,b) that belongs to Zq . Using the above elements the authority computes x=H(a),A=ga,e(g,g)b.The master key(a,x,b) is kept secretely and the remaining parameters are revealed parameters=(q,g,G,GT,e,H,H',h1,h2,A.e(g,g) b,Encryption()). The medical user MUi is examined thoroughly and based on this a health profile is generated according to which the users are provided with sensors and the necessary medical software is installed in the users Smartphone.

### C. Health Monitoring Under Normal Scenario

The medical user MUi chooses the current date CD and computes the session key (ski), Ski=H(ki||CD) and is given to the sensors and Smartphone. The data, rdata collected for every five minutes by the sensors are encrypted using the session key, Encrytion(ski,rdata||CD) to the Smartphone using Wi-Fi technology. The Wi-Fi technology increases the coverage. The Smartphone on receiving the encrypted data uses the session key(ski) to decrypt the data so as to process the rdata after which the data is sent to the healthcare center using 3G technology MUi||CD||encryption(ski,data||CD). The authority after receiving the processed data uses the master key (x) for computing MUi's secret key ki=H(MUi||x) and uses this to compute ski=H(ki||CD).This session key is used to recover the processed data data||CD from encrypted(ski,data||CD).The date is corrected and the authority sends the processed data to the medical professionals.

### D. Health Monitoring Under Emergency Situation

When MU0 faces an emergency such as abnormal raise in the heartbeat and becomes unconscious, then the authority at the healthcare centre monitors all these changes and act to this situation immediately by sending the medical professional according to the medical user's need. Before the arrival of the medical professional the user has to be monitored continuously for which the user's Smartphone requires high power for transmitting the user's health information due to which there are many chances that the resources in the user's Smartphone may not be sufficient.

To find if a person passing by is a medical user the medical user MU0 performs the following:

1. The user $MU_0$ chooses a random number $r \in Z_q^*$ and computes $e(g.g)^{b1}$ and $c = (c_1.c_2.c_3)$ as $c_1 = g^r$ $c_2 = A^1.h_1^{-r}$ $c_3 = h_2^{-r}$
2. When another $MU_j$ passes by the emergency location, $MU_0$ sends $c = (c_1.c_2.c_3)$ to the $MU_j$.

Once $MU_j$ receives $c = (c_1.c_2.c_3)$ he performs the following

Uses his access control key

$ak_j = (g^{b+ar_{j1}}.g^{r_{j2}}.g^{r_{j2}}.h_1^{r_{j2}}.h_1^{r_{j2}})$ and computes the following

$$= \frac{e(c_1.g^{b-ar_{j1}})}{e(g^{r_{j1}}.c_2).e(g^{r_{j1}}.c_2)e(h_1^{r_{j1}}h_2^{r_{j2}}.c_2)}$$

$$= \frac{e(g^r.g^b.g^{ar_{j1}})}{e(g^{r_{j1}}.g^{ar}.h_1^{-r}).e(g^{r_{j2}}.h_2^{-r}).e(h_1^{r_{j1}}.h_2^{r_{j2}}.g^r)}$$

$$= \frac{e(g^r.g^b).e(g^r.g^{ar_{j1}})}{e(g^{r_{j1}}.g^{ar}).e(g^{r_{j1}}.h_1^{-r}).e(g^{r_{j2}}.h_2^{-r}).e(h_1^{r_{j1}}.h_2^{r_{j2}}.g^r)}$$

$$= \frac{e(g^r.g^b)}{e(g^r.h_1^{r_{j1}}h_2^{r_{j2}})^{-1}.e(h_1^{r_{j1}}.h_2^{r_{j2}}.g^r)}$$

$$= e(g.g)\,br$$

Computes the H'(e(g,g)brts in which ts is the current timestamp and send back authentication ‖ ts to MU0. After the user receives authentication ‖ ts at timestamp ts', the user MU0 checks the validity of the time interval between ts' and ts to prevent replay attack. If |ts'-ts| where is the transmission delay.MU 0 accepts authentication ‖ ts and rejects otherwise then MU0 uses the stored e(g,g)br to compute authentication' = h'(e(g,g)br|| timestamp) and checks authentication' = authentication if it fails, MU j is not authenticated as a medical user.

### *E. Analysis of benefits of opportunistic computing in mobile health care emergency*

In this section , we analyze the benefits provided by the opportunistic computing to a user who is at emergency. Let us consider that the medical professionals will arrive after a time period t1 to help a user in emergency. Assuming that the users arrival follows a poisson distribution{N(t1),t1≥0} the rate of arrival of the user is taken as µ.The number of other users who are eligible to help a user at emergency is given as Nh(t1)=n0 and the number of users who pass by that scenario but are not eligible to help is given as Nħ(t1)=n1.Therfore the total number of users who arrive at the scenario before the arrival of the ambulance with the medical professionals between the time period t0 and t1 could be n0+n1. The probability that a user arriving at time can help a user at emergency is P().

***Theorem 1:***

The number of medical users who are expected to contribute resources within $[t_0.t_1]$ is $E[N_{\hbar}(t_1)] = \mu t_1 p$ Where $p = {}^{1}/_{t}.\int_{t_0}^{t_1} p(\tau)\, d\tau$

***Proof:***

The total users arriving within the time period [t0,t1] is given as N(t1)=Nh(t)+Nħ(t1)=n0 + n1 and the time is uniformly distributed in the time period [t0,t1].while defining p=P{a user who arrives in[t0,t1] is a eligible person to help| N(t1)=n0+n1}, we have p=1/t1d .The users arrive independently and so P{Nh(t1)=n0, Nħ(t1)=n1 | N(t1)=n0 +n1} will give the number of users who are qualified to help during the total n0 +n1 Bernoulli's experiment.

P{ Nh(t1)=n0, Nħ(t1)=n1}

$$=\binom{n0+n1}{n0} p^{n0}(1-p)^{n1} e^{-\mu t1 \frac{\mu t1^{n0-n1}}{(n0-n1)!}}$$

$$=\frac{(n0+n1)!}{n0!n1!} p^{n0}(1-p)^{n1}.\, e^{-\mu t1(p+1-p)\frac{\mu t1^{n0}\mu t1^{n1}}{(n0-n1)!}}$$

$$=e^{-\mu t1 p\frac{(\mu t1 p)^{n0}}{n0!}}\; e^{-\mu t1\frac{(1-p)\mu t1(1-p)^{n1}}{n1!}}$$

The above equation indicate that both Nh( and Nħ( ) are independent poisson process and their rate is $\mu t1p$ and $\mu t1(1-p)$ .Hence the number of users who are expected to help a medical user in emergency by contributing their resources is given as

$E[N_{\hbar}(t_1)] = \mu t_1 p$ Where $p = {}^{1}/_{t}.\int_{t_0}^{t_1} p(\tau)\, d\tau$

***Theorem 2:***

The resources that are expected to be contributed by the medical users who are eligible to help a user in emergency is$\frac{\mu t_1^2 p}{2}.\gamma$.

***Proof:***

Consider if the jth helper arrive at the time to the emergency location then the total resources R(t1) that can be contributed by all the helpers who are qualified is given as

$\sum_{j=1}^{N_{\hbar}(t1)}(t_1-\tau_j).\gamma$ since

$=E\{R(t_1|N_{\hbar}(t_1)=n_0\}$

$=\mathrm{E}\{\sum_{j=1}^{N_{\hbar}(t1)}(t_1-\tau_j).\gamma\,|N_{\hbar}(t_1)= n_0\}$

$=\mathrm{E}\{\sum_{j=1}^{n_0}(t_1-\tau_j).\gamma\,|N_{\hbar}(t_1)= n_0\}$

$=n_0 t_1\gamma-\mathrm{E}\{\sum_{j=1}^{n_0}\tau_j\,.\gamma\,|N_{\hbar}(t_1)= n_0\}$

$=n_0 t_1\gamma-\frac{n_0 t_1\gamma}{2}$

$=\frac{n_0 t_1\gamma}{2}$

From Theorem 1 we know that

$E(N_{\hbar}(t_1))=\mu t_1 p\;\; E[R(t_1)]$

$=\sum_{n_0=0}^{\infty}(p\{N_{\hbar}(t_1)=n_0\}|E\{R(t_1)N_{\hbar}(t_1)=n_0\})$

$=\sum_{n_0=0}^{\infty} p\{N_{\hbar}(t_1)=n_0\}.\frac{n_0 t_1\gamma}{2}$

$=\frac{t_1\gamma}{2}.E(N_{\hbar}(t_1))=\frac{\mu t_1^2 p}{2}.\gamma$

$=\mathrm{E}\{\sum_{j=1}^{n_0}(t_1-\tau_j).\gamma\,|N_{\hbar}(t_1)= n_0\}$

$=n_0 t_1\gamma-\mathrm{E}\{\sum_{j=1}^{n_0}\tau_j\,.\gamma\,|N_{\hbar}(t_1)= n_0\}$

$=n_0 t_1\gamma-\frac{n_0 t_1\gamma}{2}$

$=\frac{n_0 t_1\gamma}{2}$

### *F. Advantages*

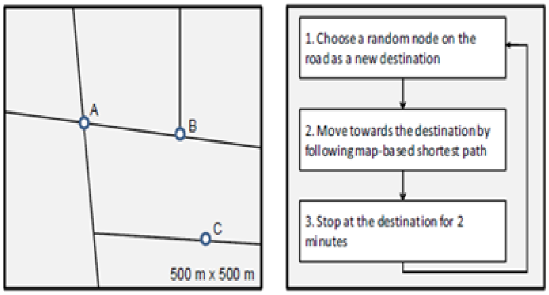
- CAM framework allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming data.
- The user-centric privacy access control to allow only those qualified helpers to participate in the opportunistic computing to balance the high-reliability of data.
- The attributed-based access control can help a medical user in emergency to identify other medical users.

## IV. RELATED WORK

The opportunistic computing has increased the great interest recently, and we have briefly reviewed them which are related to our work [2], [4], [5]. In [4], Avvenuti et al have introduced the concept of opportunistic computing in wireless sensor network which solves the problem of storing and executing an application incase if it exceeds the memory available on a single node. The application code can be partitioned in a number of simple modules that opportunistically cooperate to carry out a complex task And each node executes the provided application by running the given tasks and providing service to the neighboring nodes. In [5], Conti deals with the Opportunistic exploitation of (pools of) resources. The nodes can be able to communicate even if a completed connected path never exits between them. Mobility of the nodes provides them the opportunity to communicate with each other. Each user can avail not only of the resources available on its own device, but can also on other resources of the environment. In [2] Pazzi provides that the health information is monitored by the Sensors the sensed data to the health center using neighbor nodes. This can be transmitted to the health care centre only when there is a proper cooperation between the neighbor nodes. Although [4] and [5] are important for understanding how the concept of opportunistic computing paradigm work when resources available on other neighboring nodes to complete the given task, they have not considered the security and privacy issues existing in the opportunistic computing .Different from all the above works, our proposed PPSPC framework aims at the security and privacy issues by providing encryption.

## V. EXPERIMENTAL WORK

The health care monitoring is very important during m-Healthcare emergency with minimal privacy disclosure in today's world. The output will be then collected from sensors and they are transmitted to the user's smart phone through Wi-Fi, it is then transmitted to the health care centre by means of 3g transmission. In case of any failure in the smart phone such as when it gets switched off, the Wi-Fi router will search for other medical user's smart phone to transmit the data to the health care centre by means of opportunistic computing paradigm. This information is passed to the Health care centre for every 5 minutes under normal conditions and for every 10 seconds during the emergency conditions. Once the information reaches the health care centre, medical professional who continuously monitors the health information about the medical user will aid them at the emergency situation by sending the professional at the emergency location or by providing the ambulance. so it always provides us with the best way to find the help of users where they have been located near by the place of where the user at emergency is located. Extensive simulation results show that the proposed framework can help medical users to an great extent so users can obtain better monitoring environment.


A
B
C
500 m x 500 m
1. Choose a random node on the road as a new destination
2. Move towards the destination by following map-based shortest path
3. Stop at the destination for 2 minutes

(a) Simulation area (b) Mobility model

Fig. 2 (a) Simulation area and Fig. 2(b) Mobility model under consideration

### A. Simulation Setup

In the simulations, total l users U = {U0, U1, • • • , Ul−1} are first uniformly deployed in an interest area of 500 m×500 m, as shown in Fig. 2(a). Each user Ui ∈ U is equipped with his personal BSN and a smartphone with a transmission radius of 20 meters, and independently moves along the road with the velocity v ∈ [0.5, 1.2]m/s in the area by following the mobility model described in Fig. 2(b). Assume that the symptom character space n = 16, each user is randomly assigned 6-8 symptom characters.

TABLE I
SIMULATION SETTINGS

| parameter | Setting |
|---|---|
| Simulation area | 500m×500m |
| Simulation warm-up, duration | 10minutes,20minutes |
| Number, velocity of users | L={40,00}, v=0.5-1.2m/s |
| Similarity threshold | th={3,5} |
| Transmission of smartphone, BSN | 20m, 20m |
| Raw PHI data generation interval | Every 10 seconds |
| Emergency location | A,B, and C |

### B. Simulation Results

In the fig 3(a,b,c,d) we compare the average NQHs at locations A, B and C varying with time from 2 minutes to 20 minutes under different user number l and threshold th. From the figure, we can see, with the increase of time, the average NQH will also increase, especially for the location A. The reason is that, when all users move in the simulation area by following the same mobility model, location A will have higher traffic than locations B and C. In addition, when the user number l in the simulation area increases, the user arrival rate at locations A, B, and C also increase. Then, the average NQH increases as well. By further observing the differences of the average NQH under thresholds $th$ =3 and $th$ = 5, we can see the average NQH under $th$ = 5 is much lower than that under $th$ = 3, which indicates that, in order to minimize the privacy disclosure in opportunistic computing, the larger threshold should be chosen.

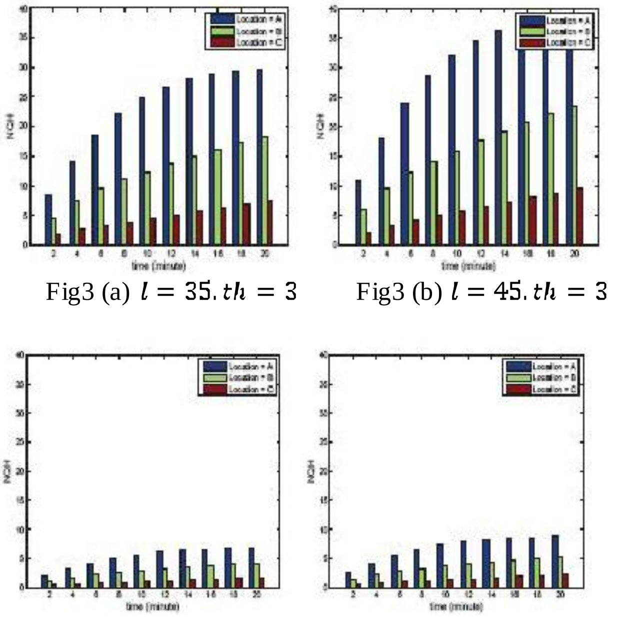


Fig3 (a) $l = 35. th = 3$ Fig3 (b) $l = 45. th = 3$

Fig3 (c) $l = 35. th = 5$ Fig3 (d) $l = 45. th = 5$

Fig 3 (a,b,c,d) NQH varying with time under number $l$ and threshold $th$

We plot the corresponding RCR varying with the time under different user number $l$ and threshold $th$. From the figure, we can observe both high-traffic location, i.e., location A, and large number of users, i.e., $l$ = 45, can reduce the U0's RCR. However, the RCR under $th$ = 5 is higher than that under $th$ = 3. Therefore, once U0 sets the threshold $th$ = 5 while the residual energy in his smartphone is not enough, his smartphone cannot support high-reliability of PHI process and transmission before the ambulance arrives.

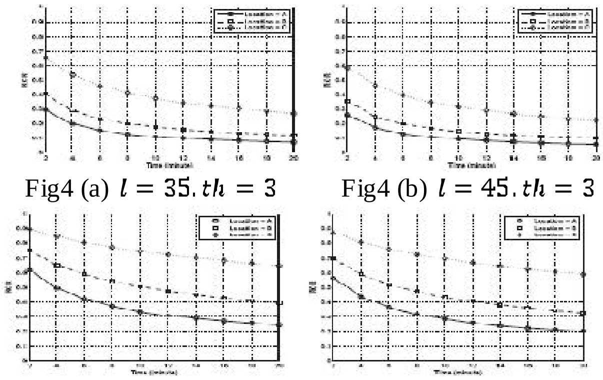


Fig4 (a) $l = 35. th = 3$ Fig4 (b) $l = 45. th = 3$

Fig4 (c) $l = 35. th = 5$ Fig4 (d) $l = 45. th = 5$

Fig 4 (a,b,c,d) RCR varying with the time under different user number $l$ and threshold $th$

## VI. FUTURE WORK

The Smart phones that are available today are open to every individual and can be programmed easily.

## VII. CONCLUSION

This paper discusses the importance of using a secure and privacy preserving opportunistic computing (CAM) framework for m-Healthcare emergency, which mainly exploits how to use opportunistic computing to achieve high reliability of process and transmission in emergency. The security issues of PPSPC with internal attackers, where the internal attackers will not honestly follow the protocol.

## ACKNOWLEDGMENT

The author would like to thank The Principal Dr. Suresh.L Cambridge Institute of Technology for giving him the opportunity to work on this project. He would like to show his sincere gratitude to his guide Prof. Janardhan Singh.K for his guidance and knowledge without which this paper would not be possible. He provided me with valuable advice which helped me to accomplish writing this paper. He is also thankful to his HOD Dr. Satyanarayanreddy.K (Department of MCA, MTECH (CSE, CNE)) for his constant encouragement and moral support.

Also he would like to thank Prof. Raghavendra.T.S for his support and encouragement, which helped me in correcting my mistakes and proceed to complete the paper with the required standards.

## REFERENCES

[1] Toninelli, R. Montanari, and A. Corradi, “Enabling secure service discovery in mobile healthcare enterprise networks,” IEEE Wireless Communications, vol. 16, pp. 24–32, 2009.
[2] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure handshake with symptoms- matching: The essential to the success of mhealthcare social network,” in Proc. BodyNets’10, Corfu Island, Greece, 2010.
[3] Y. Ren, R. W. N. Pazzi, and A. Boukerche, “Monitoring patients via a secure and mobile healthcare system,” IEEE Wireless Communications, vol. 17, pp. 59–65, 2010.
[4] R. Lu, X. Lin, X. Liang, and X. Shen, “A secure handshake scheme with symptoms- matching for mhealthcare social network,” MONET, vol. 16, no. 6, pp. 683–694, 2011.
[5] M. R. Yuce, S. W. P. Ng, N. L. Myo, J. Y. Khan, and W. Liu, “Wireless body sensor network using medical implant band,” Journal of Medical Systems, vol. 31, no. 6, pp. 467–474, 2007.

## BIOGRAPHY

**M.B.Sushrutha** is an M.Tech student of CAMBRIDGE INSTITUTE OF TECHNOLOGY, Bangalore, India Presently he is pursuing his M.Tech [CSE] from this college and he received his B.Tech from Ballari Institute of Technology & Management, affiliated to VTU University, Bellary in the year 2012. His area of interest includes Cloud computing and Object oriented Programming languages, all current trends and techniques in Computer Science.