Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Privacy Preserving Support for Mobile Health Care using Message Digest

Shireesh Kumar Manda,
Dept. of Computer Science & Engg.,
M.Tech, Software Engineering,
Kakatiya Institute of Technology & Science,
Kakatiya University, Warangal, AP, India.

B.Hanmanthu
Dept. of Computer Science & Engg.,
Assistant Professor,
Kakatiya Institute of Technology & Science,
Kakatiya University, Warangal, AP, India.

Abstract— Today we have an abundant increase in the development of Science and Technology, which in-turn made The Humans even to carry a Mini-Computer in their Palms with Screen touch, Ex: Smartphone's & Tablets etc., and parallel with the rich Enhancement in the Wireless Body Sensor Networks, it is quite useful to the Enrichment of the Medical Treatment to be very flexible, comfort via Smart Phones through the networks (2G & 3G) carriers and made the treatment very easy even to the Common person in the society with the less payable money. With these the Healthcare Authorities can treat the Patients (medical users) remotely where the patients reside at home or at various places they work. This type of a treatment can be comes under M-Healthcare (Mobile- Healthcare). Although in the m-healthcare service there are many security and data privacy problems to be overcome. Here we have A Secure and Privacy- Preserving Opportunistic Computing Framework called SPOC, for Mobile-Healthcare Emergency. Using the Smartphone and SPOC, the resources like computing power and energy can be gathered opportunistically to process the intensive Personal Health Information (PHI) of the medical user when he/she is in critical situation with minimal privacy disclosure. And also we introduce an efficient user-centric privacy access control in SPOC framework which is based on attribute access control and a new privacy-preserving scalar product computation (PPSPC) technique and makes a medical user (patient) to participate in opportunistic computing in transmitting his PHI data. Elaborated security analysis describes that the proposed SPOC framework can efficiently achieve user-centric privacy access control in M-Healthcare emergency. In this paper we introduce Privacy-Preserving Support for Mobile Healthcare using Message Digest where we have used MD5 algorithm instead of AES, which can certainly achieves an efficient way and minimises the memory consumed and the large amount of PHI data of the medical user (patient) is reduced to a fixed amount of size compared to AES which parallely increases the speed of the data to be sent to TA without any delay which in-turn the professionals at Healthcare centre can get exactly the current medical user PHI data and can save their lives in required time . As well as the algorithm is provided tight security in transmitting the patients PHI to TA. In respective performance evaluations with extensive simulations explains the MD (message digest) effectiveness in-term of providing high-reliable Personal Health Information (PHI) process and transmission while reducing the privacy disclosure during Mobile-Healthcare emergency.

Keywords— Healthcare, Computing, Privacy Preserving, Message Digest, Mobile-Healthcare, Remote Healthcare.

I. INTRODUCTION

Today in the world we have an abundant development the side of the Science and Technology. By which comparatively increased in the enrichment of the Body Sensor Nodes (BSN), Smartphone's, and sensor networks. The Medical field achieved a lot of improvement and advancement in saving the Humans lives using the latest technology based on the body sensor nodes, body sensor networks and Smartphone's. The sensor nodes are made in a small miniaturised size which can be easily placed and implanted to the patient's body and with these the patient or the medical user can attain a high quality of the medical healthcare remotely by monitoring at the healthcare centre by a Trusted Authority (TA). The above scenario can come under the mobile healthcare system (m-healthcare).

The m-healthcare is completely and purely remote based monitoring to the people who are regularly affected from the Chronic medical problems like, heart diseases and diabetes [1][2][3][4][5]. In general the patients have to wait for a longer period of time losing their important things to be done at this particular time spending at the hospitals and clinics, where as in m-healthcare system the patients (medical users) who are registered at the healthcare centre and implanted the sensor nodes and appended with a Smartphone device can be easily monitored remotely and there is no need of wasting their valuable time here and they can move anywhere they require and can have their works be done. Likewise the medical user (patient) can achieve a high quality medical healthcare remotely. The professionals at the healthcare centre are supposed to monitor the patient's condition at regular intervals of time.

© 2013, IJARCSSE All Rights Reserved

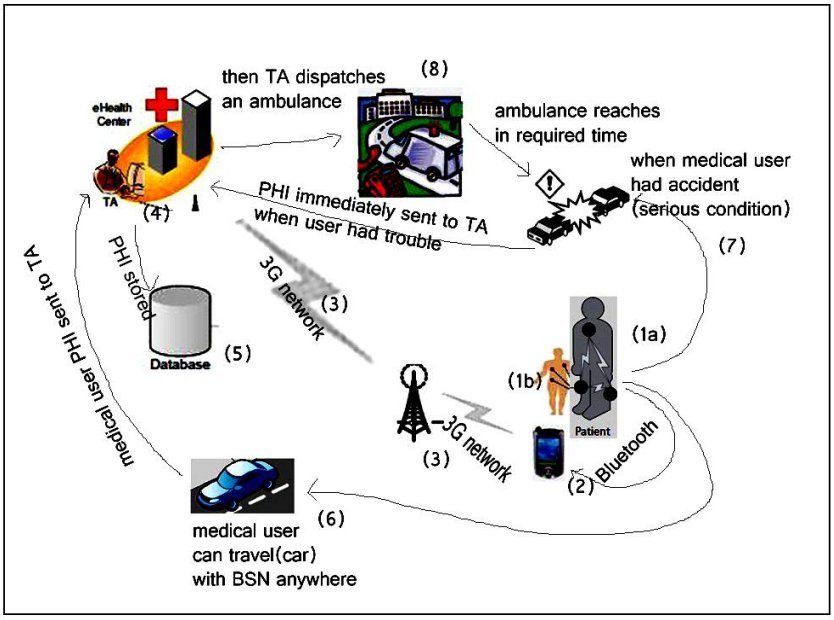

Fig 1. Overall System consideration

For Example, as shown in the figure 1. The patient who is suffering or facing from chronic diseases such as heart attacks and diabetes he/she has registered at the healthcare centre available. Once the patient is registered he/she is to be treated as a medical user like which there can be a n number of medical users registered and for each user there given a user id by which the trusted authority (TA) at the healthcare centre monitors the PHI data periodically. The medical user registration if completed he/she can be implanted to body wearable miniaturised body sensor nodes and a Smartphone device with the software appended in it. Now the patient can move to a place where he/she decides at anytime and can achieve a high quality medical treatment. The sensor nodes (BSN) which are implanted to body gathers all the typical readings at first as minimum such as heart beat, blood sugar level, blood pressure and body temperature etc, and via Bluetooth transmits to the mobile device and then transmitted to the healthcare centre via 3G networks with the user id. The healthcare centre professionals can identify the readings of which medical user is sent and when the user in emergency required actions taken by sending an ambulance and a medical representative with the vehicle and can protect the user life and thus the medical user can achieve a high quality medical healthcare service.

When the medical user is at normal situation [6] the sensor nodes can send the PHI data readings to the healthcare centre for every 10 minutes of regular intervals of time and if the patient (medical user) situation is serious then the body sensor nodes are in busy getting the readings from the patient's body in less period of time and transmit a huge and large amount of data for every 5-10 seconds in regular time intervals. Where the medical user provided Smartphone is used as a normal phone like we can use it for phoning, chatting, playing videos, listening music and browse internet..due to which the resources of the mobile like power, battery gets lowered and in emergency happens unfortunately and it might happen at low probability. i. e., 0. 005, for any medical emergency, when all of us take in to 10, 000 emergency cases into account, the common event amount will reach 50, that's not minimal and outstandingly indicates the actual reliability regarding m-Healthcare system is demanding throughout emergency.

From the above figure it clearly depicts the following:

(1a) → indicates that a patient when after registers for remote monitoring in TA he was assigned BSN into his body (1b) shows the same sensor nodes inserted to a patient. Likewise a number of patients get registered and implanted sensor nodes.

(6) and (7) → indicates that the patient can travel anywhere like the other humans without any difficulty.

The patient's readings gathered by the mobile device via Bluetooth as shown in (2). The Bluetooth sends all the data of the user in a secured way via 3G networks to the medical healthcare centre who monitors is a trusted authority as shown in (3) and (4).

Where the medical user's data is monitored and checked by the TA and securely stored in a database as shown in (5).

Medical user when met with a critical situation or with an accident and the readings are not normal as shown in (7) according to that the medical representatives knows the patient is in serious based on the readings and dispatches an ambulance within the required time and tries to save his/her life and protects him/her from the danger in major of the incidents as shown in (8).

II. PREVIOUS WORK

System Initialization

For a single-authority in m-Healthcare program under consideration, we arrange a trusted authority stated at the healthcare centre will bootstrap the entire system. Especially, by giving the security parameter, TA first attains the bilinear parameters; and selects a secure symmetric encryption, i.e., **AES**, and two secure cryptographic hash functions H and H0 . In addition, TA chooses two random numbers as the master key, two random elements in GG, and computes b.

© 2013, IJARCSSE All Rights Reserved

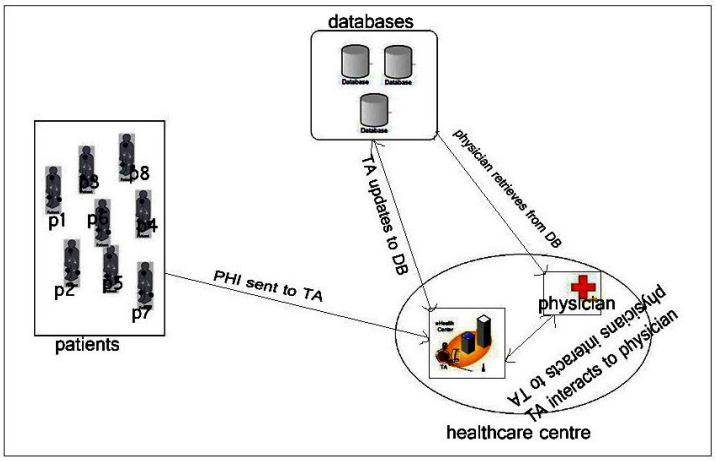

Fig 2: data communication through whole system

Here in system initialization the algorithm used is **AES**, as the algorithm cannot transmit the PHI data of a medical user who is in a critical situation. At this particular time the sensor nodes are too busy in getting the readings from the body nodes and produce a huge amount of data within a less period of time which the **AES algorithm** is not ready to encrypt and it takes a lot of time to be sent and occupies a large memory. In critical section the user data is to be sent without any delay so that they could help the user in time to save or protect his/her life, so we go for the MD5 (message digest) algorithm which encrypts the large size of data to a fixed amount of size and without any delay the data is transmitted to the healthcare centre, so through which the patient life is protected. This could be explained in the Proposed System clearly.

In M-Healthcare system, patient's PHI is always considered being reported to the e-Health centre directly, and the primary security issue is to keep the patient's PHI secret, and only the related medical professionals at e-Health centre can read them. However, due to patient's mobility, patients can often contact with each other in m-Healthcare system. If two patients have the same symptom, it is possible for them to share their health condition and experiences, provide mutual support and inspiration to each other to eliminate loneliness. We call such kind of social contact as m-Healthcare social network (MHSN).[7]

III. PROPOSED SYSTEM

Bilinear Pairings

Let GG and GGT be two multiplicative cyclic groups with the same prime order q. suppose GG and GGT are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map. In group GG, the Computational Diffie-Hellman (CDH) problem is hard; it is intractable to compute gab in a polynomial time. However, the Decisional Diffie-Hellman (DDH) problem is easy, it is easy to judge.

System Initialization

For a single-authority in m-Healthcare program under consideration, we arrange a trusted authority stated at the healthcare centre will bootstrap the entire system. Especially, by giving the security parameter, TA first attains the bilinear parameters; and selects a secure symmetric encryption, i.e., **MD5**, and two secure cryptographic hash functions H and H0 . In addition, TA chooses two random numbers as the master key, two random elements in GG, and computes b.

In 'previous work' we choose a secure symmetric encryption algorithm enc () i.e., AES, but instead here in the 'Proposed work' we use **MD5 algorithm** which is enhancement to the AES. Where as in the AES the PHI data of the medical user collected by the sensor nodes at the emergency situation is a large amount of data within a less period of time and the AES having to encrypt the PHI data is very delay and lot of time and memory space is wasted and by which the TA is unable to view the current status of the medical user. But where as in using the MD5, the time and memory utilised is reduced and it generates the PHI data of large amount to a required fixed size encryption and without any delay the data is accordingly sent to the healthcare centre and the professionals can view the exact data of the medical user and can monitor without any difficult at emergency times which is important here in these service to protect the humans lives.

Finally, TA keeps the master secretly, and publishes the system parameter. Assume there are total n symptom characters considered in m-Healthcare system, and each medical user's symptoms can be represented through his personal health profile, by a binary vector in the n-dimensional symptom character space, where ai = 1 if the medical user has the corresponding symptom character, and ai = 0 otherwise. The medical professionals at healthcare center first make medical examination for Ui, and generate Ui's personal health profile. Afterward, the following steps will be performed by TA.

- Depending upon Ui's personal health information, TA first selects the exact body sensor nodes to govern Ui's personal BSN, and installs the required medical software's in Ui's Smartphone device.
- Then, TA selects two random numbers and performs to compute the access control key for Ui.
- Finally, TA uses the master key b to compute the secret key.

© 2013, IJARCSSE All Rights Reserved

Once the patient has been implanted with the BSN and key materials will securely report his PHI to healthcare centre for attaining good healthcare monitoring by the below procedure:

- Ui first selects the current date CDate, computes the session key for a single day, and distributes the session key ki to his personal BSN and Smartphone device.
- For every five minutes, BSN gathers the raw PHI data and sends the encrypted results; to the Smartphone device.
- On getting the Smartphone device uses ki to recover rPHI from Enc;. After performing rPHI, the Smartphone device uses the 3G technology to submit the performed PHI data undergone to healthcare center.
- When the TA receives Ui at the healthcare center, he first goes with the master key b to compute Ui's secret key ski, and uses ski to compute the current session key ki. After performing that, TA uses ki to recover PHI from Enc. If the recovered CDate is corrected, TA sends PHI to the medical representatives for monitoring.

User-Centric Privacy Access Control for m-Healthcare Emergency

When a critical situation happens to medical user in m-Healthcare, e.g., user U0 accidentally fell with in no time as not usual, the healthcare representatives will handle and controls that patient's situation, and thereafter in emergency an ambulance and a medical representative will be sending to the respective place. Usually the vehicle will be dispatched nearly 15 to 20 minutes. Meanwhile the medical representative requires high-intensive PHI to real-time monitor U0. Howsoever, the energy of U0's Smartphone device may not be flexible to engage in the high-intensive PHI process and transmission. At this time, the opportunistic computing, as shown in Fig. is launched, and the below user-centric privacy access control is processed to reduce the PHI privacy exposure in opportunistic computing.

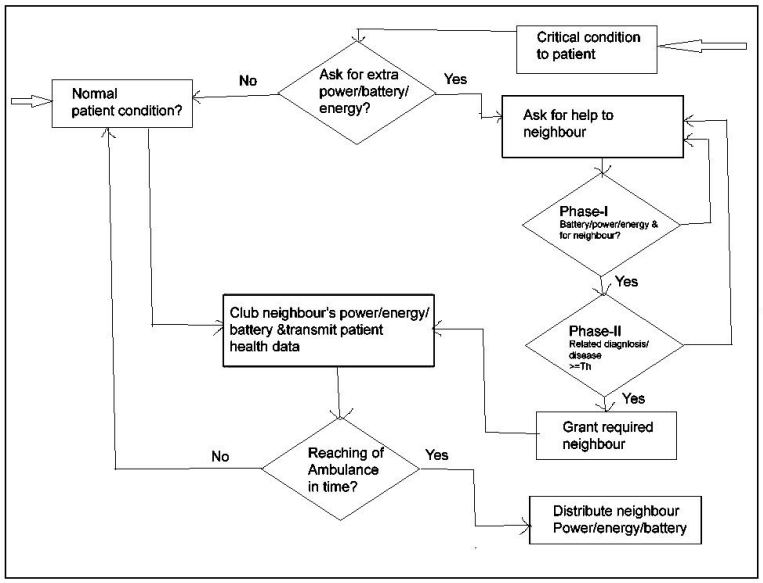

Fig: 3 Computing opportunistically for 2-phase privacy access control for Patient's critical condition and patient normal condition

Phase-I access control: The aim of phase-I access control is to locate if any other medical patient is in emergency. To attain the phase-I access control, U0's Smartphone device first selects a number which is random, when patient Uj goes by the emergency place, U0 sends CData. After receiving CData, Uj will process the below steps:

- Uses pass by person's access control key akj to compute Data;
- Compute Auth, where timestamp is the current timestamp, and returns Authktimestamp to U0. When user U0 receives Authktimestamp at time timestamp0, he first checks the validity of the time interval between timestamp0 and timestamp in order to resist the replaying attack. Once Authktimestamp is permitted, U0 accepts the Auth0. If it does hold, Uj is authenticated as a medical patient, and allows the phase-I access control.

Phase-II access control: Once Uj passes the phase-I access control, U0 and Uj will continue to process the phase-II access control to see whether they both had nearby signs to expose PHI. Let the personal health information of medical patient's U0, Uj. U0 first defines an expected threshold th for the number of common signs. Then, in order to compute a privacy-preserving route, U0 and Uj. Since the PPSPC protocol ensures neither U0 nor Uj will expose their personal healthcare information to one another during the computation it can efficiently attain privacy preserving access control.

IV. RESULTS

The concept of this paper is implemented and different results are shown below, the propose paper's concepts shows efficient results and has been efficiently tested on different Datasets.

The results shown below in Figure 4, 5, & 6, are performed on various datasets and are picturised according to the results obtained.

© 2013, IJARCSSE All Rights Reserved

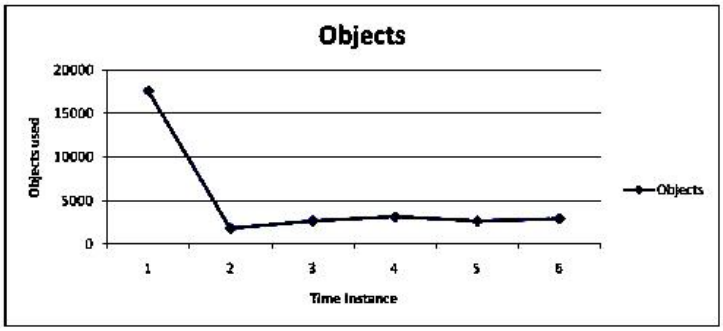

Fig. 4 Time taken by Node to initialize by objects.

Here fig.4 graph is obtained by taking under considerations of the number of datasets to be taken for a particular time instance.

Likewise a number of datasets for a six time instances, for every single time instance a lot of datasets are performed, as per the data obtained the graph is drawn.

Time Instance	Objects
1	17632
2	1800
3	2659
4	3137
5	2629
6	2892

Here in fig.5 the graph drawn shows a relation between the time instances and the memory used.

Similar as the above graph the datasets are to be considered for every single time instance and six instances are taken for our convenience.

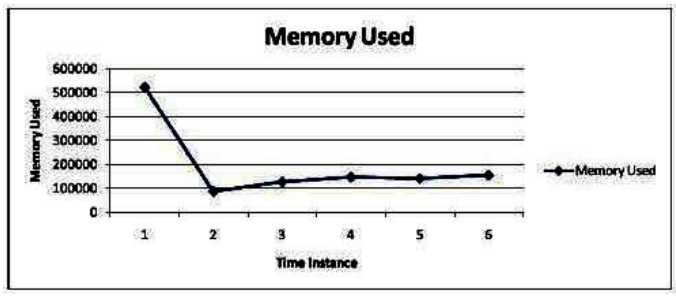

Fig.5 Time taken by Node to compute Memory Used

The above graph and the table describe the amount of memory utilized at different instance of time. Initially at the start of the sensor nodes and the smart phone since smart phone has limited memory and memory has to be allocated for creation and computation of profiles, sessions keys as well as computation of authentication timestamps there will be large amount of memory used. Then after the initialization of keys the amount of memory used will drop. And after subsequent instances of time the memory used will be very much less compared to first instance. There fore in the graph we observe that at the first instance the graph is at peak and then it drops drastically and stablize with almost smooth line which displays the amount of memory used in bytes.

Time Instance	Memory Used
1	523752
2	86660
3	127072
4	146904
5	141544
6	154596

The fig.6 indicates the graph related to the time instances and the free memory that is left. The above fig.4 clearly depicts the graph of the instances that are used by each and every single node and the objects whereas in fig.5 it shows the graph between the time instances of each and every single node and the memory utilised.

© 2013, IJARCSSE All Rights Reserved

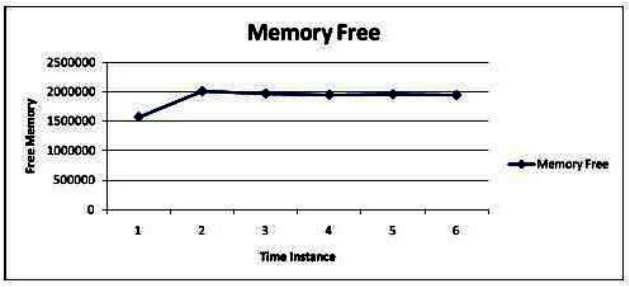

Fig. 6 Time taken by Node Communicating and Free Memory

Time Instance	Memory Free
1	1573400
2	2010492
3	1970080
4	1950248
5	1955608
6	1942556

The above graph and the table describe the amount of memory free in the smart phone at different instance of time. Initially at the start of the sensor nodes and the smart phone since smart phone has limited memory and memory has to be allocated for creation and computation of profiles, sessions keys as well as computation of authentication timestamps there will be less amount of memory free. Then after the initialization of keys the amount of memory remaining will increase. And after subsequent instances of time the memory free will be very much more compared to first instance. There fore in the graph we observe that at the first instance the graph is at low and then the remaining memory will increase which displays the amount of memory free or remaining in smart phone in bytes.

The proposed paper is implemented in Java technology on a Pentium-IV PC with minimum 20 GB hard-disk and 1GB RAM.

V. CONCLUSIONS

In this paper, we had explained the secure and privacy preserving opportunistic computing framework for m-Healthcare emergency, which clearly explains the usage of opportunistic computing to gain a high achievement of PHI process and transmission when in emergency and which mainly reduces the privacy exposure during the opportunistic computing. Elaborated security analysis gives that the exhibited SPOC framework will attain the efficient user-centric privacy access control. In respectively, with the extensive performance evaluation, we had demonstrated the exhibited SPOC framework which can sustain the high-intensive PHI process and transmission and reduces the PHI privacy exposure in m-Healthcare emergency. In our further work, we are able to perform on Smartphone-based experiments to identify and verify the effectiveness of the exhibited SPOC framework. Adding to this, we also will extend the security reasons of PPSPC with the internal attackers, with which the protocol is not followed by the internal hackers are not purely honest.

REFERENCES

[1] A. Toninelli, R. Montanari, and A. Corradi, "Enabling Secure Service Discovery in Mobile Healthcare Enterprise Networks," IEEE Wireless Comm., vol. 16, no. 3, pp. 24-32, June 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," Proc. Fifth Int'l Conf. Body Area Networks (BodyNets '10), 2010.

[3] Y. Ren, R.W.N. Pazzi, and A. Boukerche, "Monitoring Patients via a Secure and Mobile Healthcare System," IEEE Wireless Comm., vol. 17, no. 1, pp. 59-65, Feb. 2010.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms-Matching for mHealthcare Social Network," Mobile Networks and Applications—special issue on wireless and personal comm., vol. 16, no. 6, pp. 683-694, 2011.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Trans. Parallel and Distributed System, to be published.

[6] M.R. Yuce, S.W.P. Ng, N.L. Myo, J.Y. Khan, and W. Liu, "Wireless Body Sensor Network Using Medical Implant Band," J. Medical Systems, vol. 31, no. 6, pp. 467-474, 2007.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms-Matching for m-Healthcare Social Network," Mobile Networks and Applications—special issue on wireless and personal comm., vol. 16, no. 6, pp. 683-694, 2011.

© 2013, IJARCSSE All Rights Reserved