International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 6, June 2014)

SPOC Framework for Mobile and Healthcare Emergency

D.Sravani
M.Tech Scholar, Dept of CSE
TITS, JNTUH, AP, India

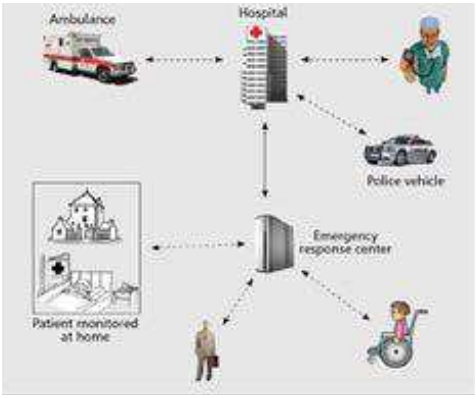
Balkrishna
Assistant Professor, Dept of CSE
TITS, JNTUH, AP, India

Abstract: **Mobile tending (m-Healthcare) system has been visualised as a vital application of pervasive computing to enhance health care quality and save lives, wherever miniaturized wearable and implantable body sensing element nodes and sensible phones square measure utilised to produce remote tending watching to those that have chronic medical conditions like polygenic disease and cardiovascular disease. User's personal health data (PHI) like heart beat, blood glucose level, vital sign and temperature et al may be initial collected by BSN. Finally, they're any transmitted to the remote tending center via electronic equipment. supported these collected letter of the alphabet knowledge, medical professionals at tending center will incessantly monitor medical users' health conditions associated additionally quickly react to users' dangerous things and save their lives by dispatching machine and medical personnel to an emergency location. The planned SPOC framework will facilitate medical users to balance the high dependability of letter of the alphabet method and minimizing the letter of the alphabet privacy speech act in m-Healthcare emergency.**

Keywords: **Healthcare, Body Sensors, Personal Health Information (PHI), Modem.**

1. INTRODUCTION:

In the current pace state of affairs, the medical world is witnessing a forceful amendment within the tending platform in terms of data digitisation to enhance health care quality and save lives. of late the smartphones square measure utilised to produce remote tending watching to those that have chronic medical conditions like polygenic disease and cardiovascular disease. Specifically in associate m-Healthcare system, medical users aren't any longer required to be monitored at intervals home or hospital environments. Instead, once being equipped with smartphone, medical users will walk outside and receive the high-quality tending watching from medical professionals anytime and anyplace.



The personal health data is inputted by the user manually by accessing the appliance on his smartphone. Then this data is accessed at the time of emergency to assign the patient to a selected doctor with acceptable specifications therein field so licensed and role specific doctors address the patients consequently. Information is maintained and accessed victimization attribute-based access management that identifies medical users in line with their specifications. For e.g. the doctor gets a distinct store house {of data knowledge} whereas a 3rd party like broker gets restricted information. Privacy conserving dot product computation (PPSPC) protocol[9] will facilitate a medical user in emergency to spot alternative medical users, and PPSPC protocol[9] will any management solely those medical users WHO have similar symptoms to participate within the timeserving computing whereas while not directly revealing users' symptoms.

As additional sensitive knowledge is shared and hold on by our medical users within the info through the web, there'll be a desire to encode knowledge hold on at these sites. One downside of encrypting knowledge is that it may be by selection shared solely at a coarse-grained level (i.e., giving another party your personal key). we tend to develop a replacement cryptosystem for fine-grained sharing of encrypted knowledge that we tend to decision Key-Policy Attribute-Based encoding (KP-ABE) . In our cryptosystem, cipher texts square measure labeled with sets of attributes and personal keys square measure related to access structures that management that cipher texts a user is ready to decipher.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 6, June 2014)

In our construction every user's secret's related to a tree-access structure wherever the leaves square measure related to attributes. A user is ready to decipher a cipher text if the attributes related to a cipher text satisfy the key's access structure. the first distinction between our setting and secret-sharing schemes is that whereas secret-sharing schemes yield cooperation between completely different parties, in our setting, this can be expressly tabu.

For instance, if a user money supply has the key related to the access structure "X AND Y", and M2 has the key related to the access structure "Y AND Z", we might not need them to be ready to decipher a cipher text whose solely attribute is Y by colluding. To do this, we tend to adapt and generalize the techniques introduced by to upset additional advanced settings. we are going to show that this cryptosystem provides North American nation a robust tool for encoding with fine-grained access management for applications like sharing audit log data.

In addition, we offer a delegation mechanism for our construction. Roughly, this enables any user that includes a key for access structure X to derive a key for access structure Y, if and provided that Y is additional restrictive than X. Somewhat astonishingly, we tend to observe that our construction with the delegation property subsumes ranked Identity-Based encoding.

Thus, implementing the attribute based mostly formula within the tending platform ends up in minimum privacy speech act that eliminates the key problems with insecure digitized data on the net.

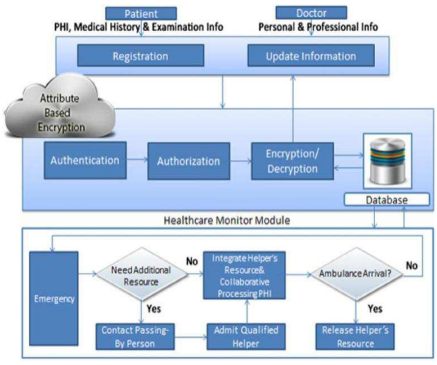
Features of planned system:

- SPOC framework[9] aims at the safety and privacy problems, and develops a user-centric privacy access management of timeserving computing in m-Healthcare emergency.
- Review the damaging effects of this state of affairs of the medical tending platform notably within the security module
- To establish mitigation alternatives which will cut back the privacy speech act problems Illustrate the variations between the prevailing and therefore the planned framework.
- Evaluate of the link between the various medical users effectively.
- Evaluate of the effectiveness of doable mitigation ways as applied within the security module, with special specialize in third-party intervention

2. SYSTEM DESIGN

In the planned system our main motive is to secure the knowledge inputted by the medical users within the system. once the users input the knowledge, it's passed to the encoding formula. we tend to develop a far richer sort of attribute-based encoding cryptosystem and demonstrate its applications. In our system, every cipher-text is labeled by associate encryptor with a group of descriptive attributes. every personal secret's related to associate access structure that specifies which kind of cipher-texts the key will decipher. we tend to decision such a theme a Key-Policy Attribute-Based encoding (KP-ABE), since the access structure is per the personal key, whereas the cipher-texts square measure merely labeled with a group of descriptive attributes. we tend to note that this setting is harking back to secret sharing schemes. Victimization notable techniques one will build a secret-sharing theme that specifies that a group of parties should get together so as to reconstruct a secret. as an example, one will specify a tree access structure wherever the inside nodes carries with it AND/OR gates and therefore the leaves carries with it completely different parties. Any set of parties that satisfy the tree will reconstruct the key. In our context, the role of the parties is taken by the attributes. Thus, the access structure A can contain the licensed sets of attributes. we tend to limit our attention to monotone access structures. However, it's conjointly doable to (inefficiently) understand general access structures victimization our techniques by having the NOT of associate attribute as a separate attribute altogether. Thus, the quantity of attributes within the system are doubled. In our construction every user's secret's related to a tree-access structure wherever the leaves square measure related to attributes. A user is ready to decipher a cipher-text if the attributes related to a cipher -text satisfy the key's access structure. Thus, provided that the user or a celebration is documented to use the information he/she is allowed for that otherwise a decrypted secret's required for it. This makes positive that the information is accessible provided that the parties provide the proper access key. Otherwise the user is denied the request of accessing the information that they have.

System Architecture



In our context, the role of the parties is taken by the attributes. Thus, the access structure A can contain the licensed sets of attributes. we tend to limit our attention to monotone access structures. However, it's conjointly doable to (inefficiently) understand general access structures victimization our techniques by having the not of associate attribute as a separate attribute altogether. Thus, the quantity of attributes within the system are doubled. From currently on, unless explicit otherwise, by associate access structure we tend to

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 6, June 2014)

mean a monotone access structure. associate (Key-Policy) Attribute based mostly encoding theme consists of 4 algorithms.

Setup: This is a irregular formula that takes no input aside from the implicit security parameter. It outputs the general public parameters PK and a master MK.

Encryption: This is a irregular formula that takes as input a message m, a group of attributes γ, and therefore the public parameters PK. It outputs the cipher text E.

Key Generation: This is a irregular formula that takes as input – associate access structure A, the master MK and therefore the public parameters PK. It outputs a cryptography key D.

Init: The human declares the set of attributes, γ, that he needs to be challenged upon.

3. SECURITY:

*Bilinear Maps:*We gift a number of facts associated with teams with expeditiously estimable additive maps. Let G1 and G2 be 2 increasing cyclic teams of prime order p. Let g be a generator of G1 and e be a additive map

LSSS and Monotone Span Programs: In a linear secret-sharing theme [4], realizing associate access structure A, a 3rd party referred to as the dealer holds a secret y and distributes the shares of y to parties such y may be reconstructed by a linear combination of the shares of any licensed set. Further, associate unauthorized set has no data regarding the key.

There is an in depth relation between LSSS and a linear algebraical model of computation referred to as monotone span programs (MSP). it's been shown that the existence of associate economical LSSS for a few access structure is appreciate the existence of atiny low monotone span program for the characteristic operate of that access structure . the subsequent definition of MSP may be a slightly altered version of the one given .

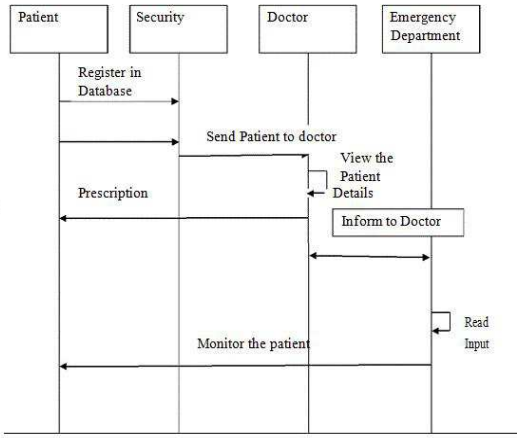
Definition (Monotone Span Program): Again, since the role of parties are assumed by attributes in our context, every row of the matrix M are labeled by associate attribute.

Construction for Access Trees: In the access-tree construction, cipher texts square measure labeled with a group of descriptive attributes. Personal keys square measure known by a tree-access structure during which every interior node of the tree may be a logic element and therefore the leaves square measure related to attributes. (We note that this setting is extremely communicative . as an example, we will represent a tree with "AND" and "OR" gates by victimization severally two of two and one of two threshold gates.) Users are ready to decipher a cipher text with a given key if associated provided that there's an assignment of attributes from the cipher texts to nodes of the tree such the tree is glad.

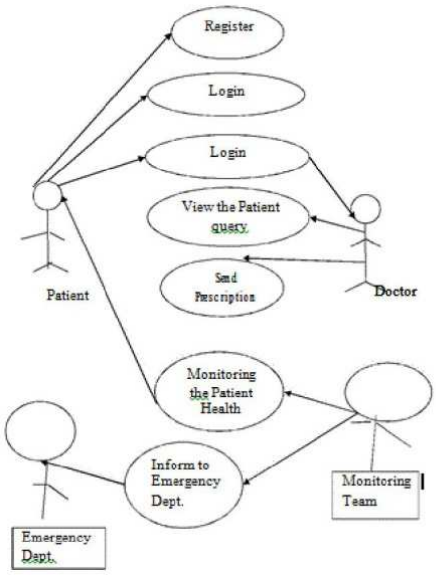
Access Tree (T): Let 'T' be a tree representing an access structure. Each non -leaf node of the tree represents a threshold gate, described by its children and a threshold value. If numx is the number of children of a node x and kx is its threshold value, then $0 < kx \leq numx$. When kx = 1, the threshold gate is an OR gate and when kx = numx, it is an AND gate. Each leaf node x of the tree is described by an attribute and a threshold value kx = 1.

To facilitate working with the access trees, we define a few functions. We denote the parent of the node x in the tree by parent(x). The function att(x) is defined only if x is a leaf node and denotes the attribute associated with the leaf node x in the tree. The access tree T also defines an ordering between the children of every node, that is, the children of a node are numbered from 1 to num. The function index(x) returns such a number associated with the node x. where the index values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner.

Sequence Diagram for the security module:



Use Case Diagram:



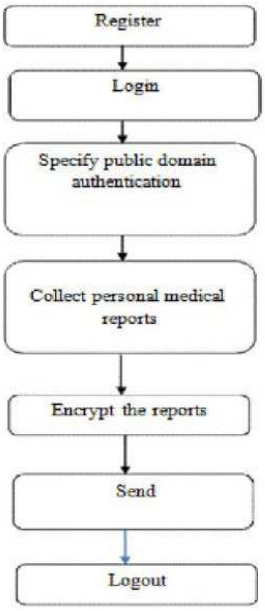
International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 6, June 2014)

4. MODULE DESCRIPTION:

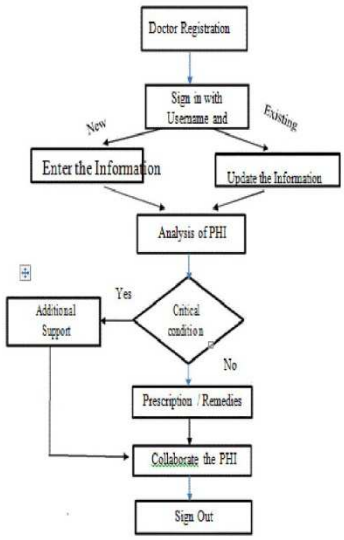
User Module: The registration includes sign up of new user into the websites. The registration may include the personal information, medical history and the examination. The personal information consists of username, password, email, phone, age, gender, height. The medical history consist owner's condition, allergies, medical prescription. The examination consists of pulse rate, heart rate, blood Test.

Security Module: In this module, the PHI is encrypted using the attribute based algorithm. A key is generated as an output in the initial step of encryption. Thus, the encrypted data called the cipher-text is accessed on the basis of attribute keys. Otherwise the access is rejected

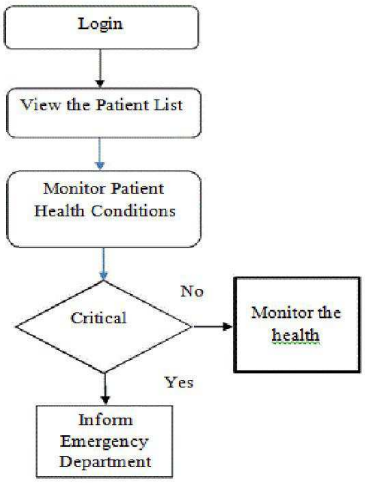
Patient Module: The Patient Module includes all the procedures and the protocols the patient has to undergo. It starts with the registration process with our web application. Next it goes up with signing the agreement of disclosing all the information about his personal health. The registration includes sign up of new user into the websites. The registration may include the personal information, medical history and the examination.



Doctor Module: The Doctor undergoes the same process of registrations in our web application. They also sign up an agreement for their availability in demanding situations. The registration includes sign up of new doctor into the websites. The registration may include the doctor's personal information as well as professional information. The professional information consists of his/her profession, specialization and his/her hospital name. Also, the doctor updates the PHI of the patient after the check-up.



Health Monitor Module:



In this module the hospitals and the control of remote centre comes into existence. Each mobile medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature and others, can be first collected by patient /patient relatives. Finally, they are further transmitted to the remote healthcare centre via modem. Based on these collected PHI data, medical professionals at healthcare centre can continuously monitor medical users' health conditions and as well quickly react to users' life-threatening situations.

5. CONCLUSION

Mobile Healthcare Emergency Platform has revolutionized the way people used to store and access their medical records. The digitization of the health information has not only saved money but also has saved additional overhead that occurred earlier. This is a new topic which is drawing attention because of the secured framework that helps user in maintaining their health information private to themselves and the other medical

users with similar symptoms so that he can be a helper in the opportunistic framework. This process is becoming more and more user-centric to let users identify and mitigate emergency cases thus helping them save lives of their close ones and others as well. The system has an attribute based encryption mechanism which limits the visibility of the information to only authenticated users thus minimizing the disclosure of information to the unauthorized ones. Since this system has evolved over the years but still it faces the threat of misuse of information. So, in this project, a secured system has been proposed to minimize the threat and thus benefit its users to a large extent. The scope of this platform is not limited and hence is an important field of research especially in terms of security.

REFERENCES

[1]. 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.
[2]. 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 andpersonal comm., vol. 16, no. 6, pp. 683-694, 2011.
[3]. 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 DistributedSystem, to be published.
[4]. 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.
[5]. M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, "Opportunistic Computing for Wireless Sensor Networks," Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '07), pp. 1-6, 2007.
[6]. A. Passarella, M. Conti, E. Borgia, and M. Kumar, "Performance Evaluation of Service Execution in Opportunistic Computing," Proc. 13th ACM Int'l Conf. Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWIM '10), pp. 291-298, 2010.
[7]. M. Conti, S. Giordano, M. May, and A. Passarella, "From Opportunistic Networks to Opportunistic Computing," IEEE Comm. Magazine, vol. 48, no. 9, pp. 126-139, Sept. 2010.
[8]. M. Conti and M. Kumar, "Opportunities in OpportunisticComputing," IEEE Computer, vol. 43, no. 1, pp. 42-50, Jan. 2010.
[9]. W. Du and M. Atallah, "Privacy-Preserving Cooperative StatisticalAnalysis," Proc. 17th Ann. Computer Security Applications Conf.(ACSAC '01), pp. 102-111, 2001,
[10]. J. Vaidya and C. Clifton, "Privacy Preserving Association Rule Mining in Vertically Partitioned Data," Proc. Eighth ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD '02), pp. 639- 644, 2002.

About the authors:

D. Sravani currently Pursuing M.Tech from **TURBOMACHINERY Institute of Technology & Sciences,** HYDERABAD, A.P, India. She received her B.Tech from Sri Kottam Tulasi Reddy Memorial College of Engineering, affiliated to JNTU in the year of 2012. Her areas of interest includes Computer Networks, Parallel and Distributed System, Data Mining, Network security.

Mr .Balkrishna is currently working as an Assistant Professor, in Department of Computer Science & Engineering in TURBOMACHINERY INSTITUTE OF TECHNOLOGY & SCIENCES, HYDERABAD, A.P, India. He has received his Masters from Acharya Nagarjuna University. He was certified in CIT Programming, he had worked as Cyber Security Workshop Coordinator. He attended for network programming &computer network workshop conducted by iit Bombay. He has research interests include Software Engineering, Mobile and Cloud computing technologies, Data Mining, Computer Networks, Network security, and Database Management Systems.