SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency.

PremMithilesh.M#1, **Mani Krishna.P**#2, **DheerajBatchu**#3 **Mrs.MrudulaOruganti**#4

[1,2] Department of Computer Science,SRMUniversity,Chennai,India.
[3]Department of Computer Science,Amrita School of Engineering,Coimbatore,India.
[4]Department of Computer Science,SRMUniversity,Chennai,India.

ABSTRACT:

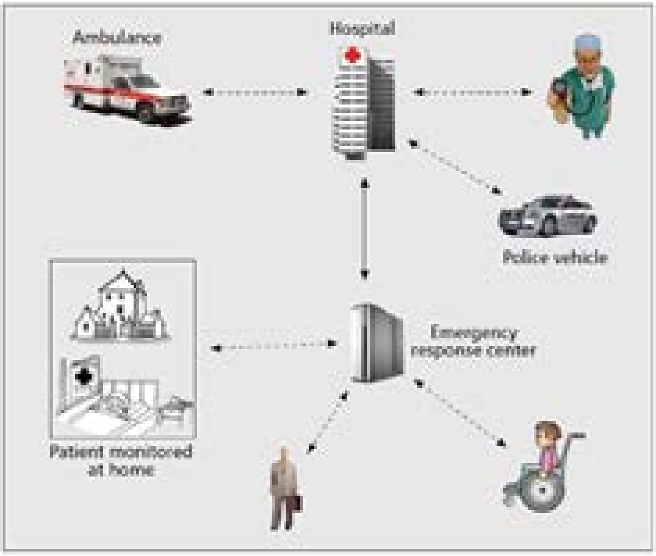
Mobile Healthcare (m-Healthcare) system has been envisioned as an important application of pervasive computing to improve health care quality and save lives, where miniaturized wearable and implantable body sensor nodes and smart phones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease. User's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature and others can be first collected by BSN. Finally, they are further transmitted to the remote healthcare center via Modem. Based on these collected PHI data, medical professionals at healthcare center can continuously monitor medical users' health conditions and as well quickly react to users' life-threatening situations and save their lives by dispatching ambulance and medical personnel to an emergency location. The proposed SPOC framework can help medical users to balance the high reliability of PHI process and minimizing the PHI privacy disclosure in m-Healthcare emergency.

KEYWORDS: HEALTHCARE, BODY SENSORS,PERSONAL HEALTH INFORMATION (PHI), MODEM.

I. INTRODUCTION:

In the current galloping scenario, the medical world is witnessing a drastic change in the healthcare platform in terms of information digitization to improve health care quality and save lives. These days the smartphones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease. Specifically in an m-Healthcare system, medical users are no longer needed to be monitored within home or hospital environments. Instead, after being equipped with smartphone, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere.

The personal health information is inputted by the user manually by accessing the application on his smartphone. Then this information is accessed at the time of emergency to assign the patient to a particular doctor with appropriate specifications in that field so that authorized and role specific doctors address the patients accordingly.



Information is maintained and accessed using attribute-based access control which identifies medical users according to their specifications. For e.g. the doctor gets a different store house of information while a third party like Insurance Agent gets limited information. Privacy preserving scalar product computation (PPSPC) protocol[9] can help a medical user in emergency to identify other medical users, and PPSPC protocol[9] can further control only those medical users who have similar symptoms to participate in the opportunistic computing while without directly revealing users' symptoms.

As more sensitive data is shared and stored by our medical users in the database through the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, cipher texts are labelled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.

In our construction each user's key is associated with a tree-access structure where the leaves are associated with attributes. A user is able to decrypt a cipher text if the attributes associated with a cipher text satisfy the key's access structure. The primary difference between our setting and secret-sharing schemes is that while secret-sharing schemes allow for cooperation between different parties, in our setting, this is expressly forbidden.

For instance, if a user M1 has the key associated with the access structure "X AND Y", and M2 has the key associated with the access structure "Y AND Z", we would not want them to be able to decrypt a cipher text whose only attribute is Y by colluding. To do this, we adapt and generalize the techniques introduced by to deal with more complex settings. We will show that this cryptosystem gives us a powerful tool for encryption with fine-grained access control for applications such as sharing audit log information.

In addition, we provide a delegation mechanism for our construction. Roughly, this allows any user that has a key for access structure X to derive a key for access structure Y, if and only if Y is more restrictive than X. Somewhat surprisingly, we observe that our construction with the delegation property subsumes Hierarchical Identity-Based Encryption.

Thus, implementing the attribute based algorithm in the healthcare platform leads to minimum privacy disclosure which eliminates the major issues of insecure digitized information on the web.

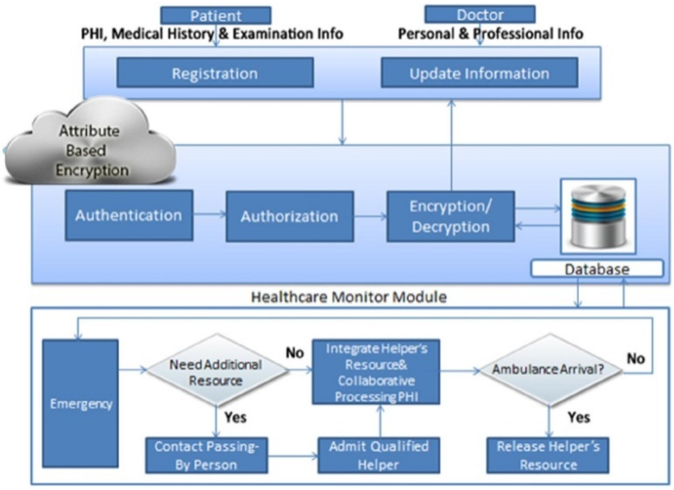
Features of proposed system:

- SPOC framework[9] aims at the security and privacy issues, and develops a user-centric privacy access control of opportunistic computing in m-Healthcare emergency.
- Review the detrimental effects of the current scenario of the medical healthcare platform particularly in the security module
- To identify mitigation alternatives that may reduce the privacy disclosure issues Illustrate the differences between the existing and the proposed framework.
- Evaluate of the relationship between the different medical users effectively[2][4].
- Evaluate of the effectiveness of possible mitigation strategies as applied in the security module, with special focus on third-party intervention

II. SYSTEM ARCHITECTURE

In the proposed system our main motive is to secure the information inputted by the medical users in the system. After the users input the information, it is passed to the encryption algorithm. We develop a much richer type of attribute-based encryption cryptosystem and demonstrate its applications. In our system, each cipher-text is labelled by an encryptor with a set of descriptive attributes. Each private key is associated with an access structure that specifies which type of cipher-texts the key can decrypt. We call such a scheme a Key-Policy Attribute-Based Encryption (KP-ABE)[5], since the access structure is specified in the private key, while the cipher-texts are simply labelled with a set of descriptive attributes. We note that this setting is reminiscent of secret sharing schemes. Using known techniques one can build a secret-sharing scheme that specifies that a set of parties must cooperate in order to reconstruct a secret. For example, one can specify a tree access structure where the interior nodes consist of AND/OR gates and the leaves consist of different parties. Any set of parties that satisfy the tree can reconstruct the secret. In our context, the role of the parties is taken by the attributes. Thus, the access structure A will contain the authorized sets of attributes. We restrict our attention to monotone access structures. However, it is also possible to (inefficiently) realize general access structures using our techniques by having the NOT of an attribute as a separate attribute altogether. Thus, the number of attributes in the system will be doubled. In our construction each user's key is associated with a tree-access structure where the leaves are associated with attributes. A user is able to decrypt a cipher-text if the attributes associated with a cipher-text satisfy the key's access structure. Thus, only if the user or a party is authenticated to use the data he/she is allowed for that otherwise a decrypted key is needed for it. This makes sure that the data is accessible only if the parties give the correct access key. Otherwise the user is denied the request of accessing the data which they need.

System Architecture:


Patient
PHI, Medical History & Examination Info
Doctor
Personal & Professional Info
Registration
Update Information
Attribute Based Encryption
Authentication
Authorization
Encryption/ Decryption
Database
Healthcare Monitor Module
Emergency
Need Additional Resource
No
Yes
Integrate Helper's Resource& Collaborative Processing PHI
Ambulance Arrival?
No
Yes
Contact Passing-By Person
Admit Qualified Helper
Release Helper's Resource

Description:

Let {P1,P2,...,Pn} be a set of parties. A collection A$\subseteq 2^{\{P1,P2,...,Pn\}}$ is monotone if ∀B,C : if B ∈A and B ⊆ C then C ∈A. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) A of non-empty subsets of {P1,P2,...,Pn}, i.e., A $\subseteq 2^{\{P1,P2,...,Pn\}}\backslash\{\emptyset\}$. The sets in A are called the authorized sets, and the sets not in A are called the unauthorized sets.

In our context, the role of the parties is taken by the attributes. Thus, the access structure A will contain the authorized sets of attributes. We restrict our attention to monotone access structures. However, it is also possible to (inefficiently) realize general access structures using our techniques by having the not of an attribute as a separate attribute altogether. Thus, the number of attributes in the system will be doubled. From now on, unless stated otherwise, by an access structure we mean a monotone access structure. An (Key-Policy) Attribute Based Encryption scheme consists of four algorithms.

Setup:

This is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

Encryption:

This is a randomized algorithm that takes as input a message m, a set of attributes γ, and the public parameters PK. It outputs the cipher text E.

Key Generation:

This is a randomized algorithm that takes as input – an access structure A, the master key MK and the public parameters PK. It outputs a decryption key D.

Decryption:

This algorithm takes as input – the cipher text E that was encrypted under the set γ of attributes, the decryption key D for access control structure A and the public parameters PK. It outputs the message M if γ ∈A.

We now discuss the security of an ABE scheme. We define a selective-set model for proving the security of the attribute based under chosen plaintext attack. This model can be seen as analogous to the selective-ID model [16, 17, 8] used in identity-based encryption (IBE) schemes.
Selective-Set Model for ABE

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

III. SECURITY:

Bilinear Maps:

We present a few facts related to groups with efficiently computable bilinear maps. Let G1 and G2 be two multiplicative cyclic groups of prime order p. Let g be agenerator of G1 and e be a bilinear map, e : G1 ×G1 →G2. The bilinear map e has the following properties:

1. Bi-linearity: for all u,v∈G1 and a,b∈Zp, we have $e(u^a,v^b) = e(u,v)^{ab}$.
2. Non-degeneracy: e(g,g) =6 1.

We say that G1 is a bilinear group if the group operation in G1 and the bilinear map e : G1 ×G1 → G2 are both efficiently computable. Notice that the map e is symmetric since $e(g^a,g^b) = e(g,g)^{ab} = e(g^b,g^a)$.

The Decisional Bilinear Diffie-Hellman (BDH) Assumption

Let a,b,c,z∈Zp be chosen at random and g be a generator of G1. The decisional BDH assumption [8, 34] is that no probabilistic polynomial-time algorithm B can distinguish the tuple $(A = g^a,B = g^b,C = g^c,e(g,g)^{abc})$ from the tuple $(A = g^a,B = g^b,C = g^c,e(g,g)^z)$ with more than a negligible advantage. The advantage of B is

$$\left|\Pr[\mathcal{B}(A,B,C,e(g,g)^{abc})=0]-\Pr[\mathcal{B}(A,B,C,e(g,g)^{z})]=0\right|$$

where the probability is taken over the random choice of the generator g, the random choice of a, b, c, z in Zp, and the random bits consumed by B.

LSSS and Monotone Span Programs:

In a linear secret-sharing scheme [4], realizing an access structure A, a third party called the dealer holds a secret y and distributes the shares of y to parties such that y can be reconstructed by a linear combination of the shares of any authorized set. Further, an unauthorized set has no information about the secret y.

There is a close relation between LSSS and a linear algebraic model of computation called monotone span programs (MSP) . It has been shown that the existence of an efficient LSSS for some access structure is equivalent to the existence of a small monotone span program for the characteristic function of that access structure . The following definition of MSP is a slightly altered version of the one presented .
Definition (Monotone Span Program):

Let K be a field and {x1,...,xn} be a set of variables. A monotone span program over K is labelled matrix Mˆ (M,ρ) where M is a matrix over K, and ρ is a labelling of the rows of M by literals from {x1,...,xn} (every row is labelled by one literal).
A monotone span program accepts or rejects an input by the following criterion. For every input set γ of literals, define the sub-matrix Mγ of M consisting of those rows whose labels are in γ, i.e., rows labelled by some xi such that xi ∈ γ. The monotone span program Mˆ accepts γ if and only if ~1 ∈ span (Mγ), i.e., some linear combination of the rows of Mγ gives the all-one vector ~1. The MSP Mˆ computes a Boolean function fM if it accepts exactly those inputs γ where fM(γ) = 1. The size of Mˆ is the number of rows in M.

Again, since the role of parties will be assumed by attributes in our context, each row of the matrix M will be labelled by an attribute.
Construction for Access Trees

In the access-tree construction, cipher texts are labelled with a set of descriptive attributes. Private keys are identified by a tree-access structure in which each interior node of the tree is a threshold gate and the leaves are associated with attributes. (We note that this setting is very expressive. For example, we can represent a tree with “AND” and “OR” gates by using respectively 2 of 2 and 1 of 2 threshold gates.) A user will be able to decrypt a cipher text with a given key if and only if there is an assignment of attributes from the cipher texts to nodes of the tree such that the tree is satisfied.

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 ≤ 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.

Satisfying an access tree: Let T be an access tree with root r. Denote by Tx the subtree of T rooted at the node x. Hence T is the same as Tr. If a set of attributes γ satisfies the access tree Tx, we denote it as Tx(γ) = 1. We compute Tx(γ) recursively as follows. If x is a non-leaf node, evaluate Tx0(γ) for all children x^0 of node x. Tx(γ) returns 1 if and only if at least kx children return 1. If x is a leaf node, then Tx(γ) returns 1 if and only if att(x) ∈ γ.

The master key MK is: *t*1,...,*t*|U|,*y* .

Encryption (M,γ,PK) To encrypt a message M ∈ G2 under a set of attributes γ, choose a random value s ∈Zp and publish the cipher text as:

$$E = (\gamma, E' = MY^s, \{E_i = T_i^s\}_{i\in\gamma}) \ .$$

Key Generation (T ,MK): The algorithm outputs a key that enables the user to decrypt a message encrypted under a set of attributes *γ* if and only if T (*γ*) = 1. The algorithm proceeds as follows. First choose a polynomial *qx* for each node *x* (including the leaves) in the tree T . These polynomials are chosen in the following way in a top-down manner, starting from the root node *r*.

For each node *x* in the tree, set the degree *dx* of the polynomial *qx* to be one less than the threshold value *kx* of that node, that is, *dx* = *kx* − 1. Now, for the root node *r*, set *qr*(0) = *y* and *dr* other points of the polynomial *qr* randomly to define it completely. For any other node *x*, set

qx(0) =*q*parent(*x*)(index(*x*)) and choose *dx* other points randomly to completely define*qx*.

Once the polynomials have been decided, for each leaf node *x*, we give the following secret value to the user

$$D_x = g^{\frac{q_x(0)}{t_i}} .$$

where*i* = att(*x*) .The set of above secret values is the decryption

key*D*.

Decryption (*E*,*D*) We specify our decryption procedure as a recursive algorithm . For ease of exposition we present the simplest form of the decryption algorithm and discuss potential performance improvements in the next subsection.

We first define a recursive algorithm DecryptNode(*E*,*D*,*x*) that takes as input the cipher text), the private key *D* (we assume the access tree T is embedded in the private key), and a node *x* in the tree. It outputs a group element of G2 or ⊥.
Let *i* = att(*x*). If the node *x* is a leaf node then:

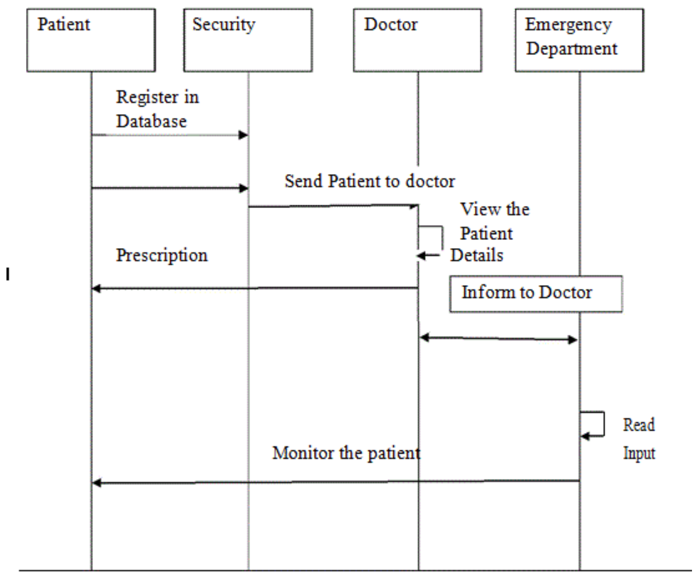
$$\mathrm{DecryptNode}(E,D,x) = \begin{cases} e(D_x, E_i) = e(g^{\frac{q_x(0)}{t_i}}, g^{s\cdot t_i}) = e(g,g)^{s\cdot q_x(0)} \text{ if } i \in \gamma \\ \perp \text{ otherwise} \end{cases}$$

We now consider the recursive case when *x* is a non-leaf node. The algorithm DecryptNode(*E*,*D*,*x*) then proceeds as follows: For all nodes *z* that are children of *x*, it calls DecryptNode(*E*,*D*,*z*) and stores the output as *Fz*. Let *Sx* be an arbitrary *kx*-sized set of child nodes *z* such that *Fz* =6 ⊥. If no such set exists then the node was not satisfied and the function returns ⊥.

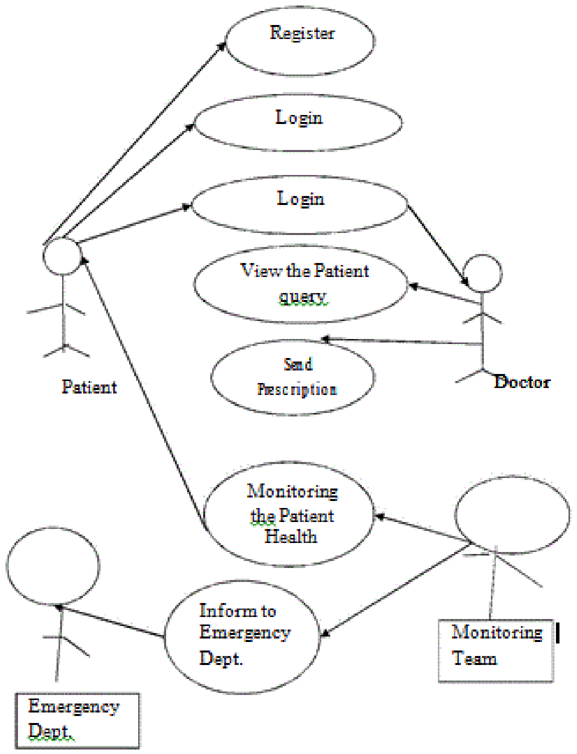
Otherwise, we compute:

$$\begin{aligned} F_x &= \prod_{z\in S_x} F_z^{\Delta_{i,S'_x}(0)}, \quad \text{where } {}^{i=\mathrm{index}(z)}_{S'_x=\{\mathrm{index}(z):z\in S_x\}} \\ &= \prod_{z\in S_x} (e(g,g)^{s\cdot q_z(0)})^{\Delta_{i,S'_x}(0)} \\ &= \prod_{z\in S_x} (e(g,g)^{s\cdot q_{\mathrm{parent}(z)}(\mathrm{index}(z))})^{\Delta_{i,S'_x}(0)} \quad \text{(by construction)} \\ &= \prod_{z\in S_x} e(g,g)^{s\cdot q_x(i)\cdot\Delta_{i,S'_x}(0)} \\ &= e(g,g)^{s\cdot q_x(0)} \quad \text{(using polynomial interpolation)} \end{aligned}$$

Sequence Diagram for the security module:



Use Case Diagram:



IV. MODULE DESCRIPTION:

. User Module:

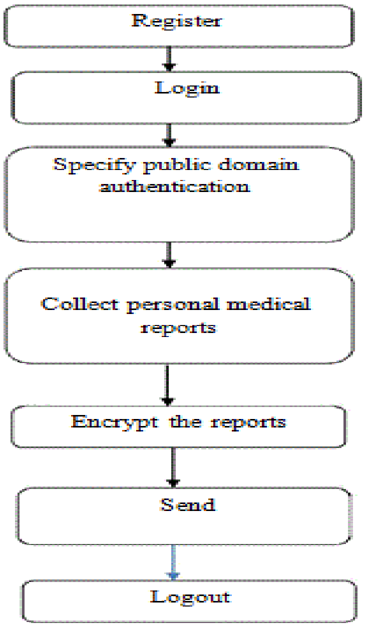
The registration includes sign up of new user into the websites. The registration may include the personal information, medical history and the examination. The personal information consists of username, password, email, phone, age, gender, height. The medical history consist owner’s condition, allergies, 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[5]. 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

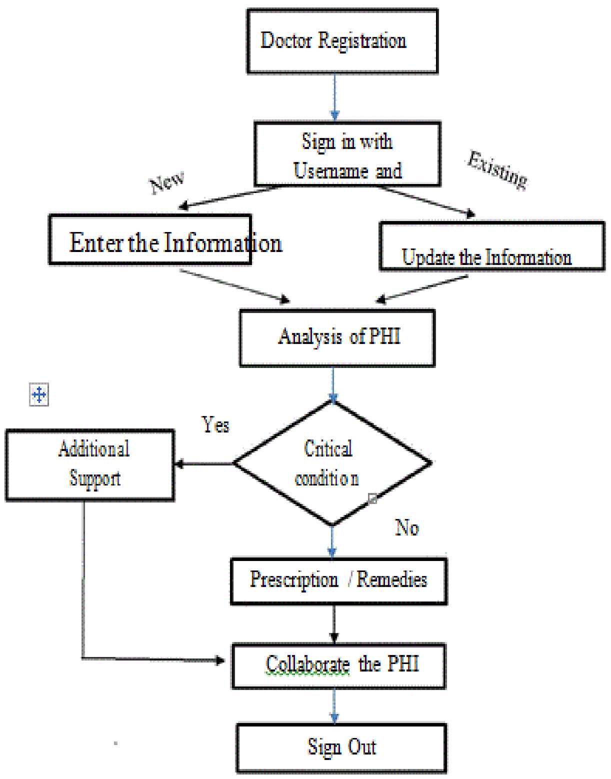
Patient Module:

The Patient Module includes all the procedures and the protocols the patient has to undergo[1]. 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.

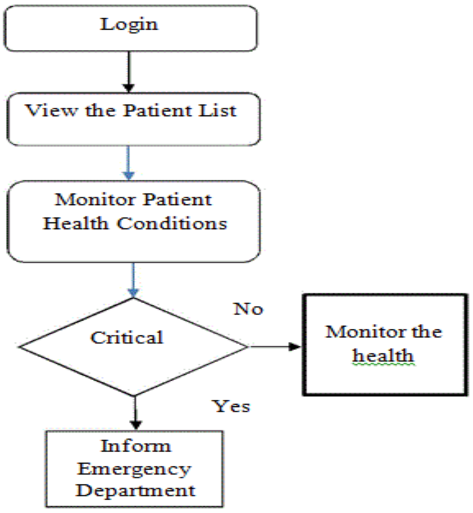

Register
Login
Specify public domain authentication
Collect personal medical reports
Encrypt the reports
Send
Logout

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[3].



Health Monitor Module:


Login
View the Patient List
Monitor Patient Health Conditions
Critical
No
Monitor the health
Yes
Inform Emergency Department

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[3]. 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.

VI. 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.

VII. FUTURE WORK

In this project, we have proposed a user-centric approach (through attribute based framework) towards mobile healthcare emergency by looking into the current security issues that make it vulnerable to access by unauthorized sources in absence of attribute based framework.

In the near future, we intend to perform experiments that are closely related to hacks and other security issues of the proposed framework. In addition, we also intend to implement other possible technological advancements including artificial intelligence in our project so that the framework can be automated completely thus minimizing the time lags a step further. In addition to this, we plan to further enhance the framework by implementing body sensors nodes[6][7][8] functionality in India as well.

VIII. ACKNOWLEDGEMENT

The paper was developed under the supervision of Dr. J.Jagadeesan, M.Tech(Ph.D) A.P(S.G)&HOD, Mr. AugustianIssac.R M.E.,A.P(Sr.G) and guidance of: Mrs. MrudulaOruganti, M.Tech A.P(O.G)..The Authors thank their support, navigation and help at different stages of the project.

IX. 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 SymptomsMatching 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] 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.

[8] 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

[9] SPOC: A Secure and Privacy-PreservingOpportunistic Computing Frameworkfor Mobile-Healthcare Emergency RongxingLu,Member, IEEE, Xiaodong Lin, Senior Member, IEEE, andXuemin (Sherman) Shen,Fellow, IEEE