# New Secure Communication Protocols for Mobile E-health System

M.Aramudhan
PKIET
Karaikal, INDIA

K.Mohan
Research scholar
Sathyabama University ,Chennai

## ABSTRACT

E-health system has been used as communication system that enables to deliver medical service over the Internet. The medical information’s accessible in e-health systems are highly sensitive and distributed that demands strong authentication and authorization mechanisms for communication between the healthcare professionals, consumers and providers. Internet is an open system that provides global access without much constraint. Hence, e-health users demand safe communication and user privacy over the Internet. This paper introduces three secure communication protocols based on message passing and Mobile agent for online e-health system. Certificate based Authentication and Attribute based Policy assigned Authorization framework (CAAPA) for mobile users is proposed based on message passing technique. Token based Cross Verification (TCV) protocol is proposed for secure services in e-health System over Internet based on Mobile agent. Secure and Auditable Agent- based Communication Protocol (SAACP) performs on key exchange mechanism with mobile agents to reduce the delay in communication. Intelligent mobile agents are proposed for negotiating the policy of the users dynamically. All the above protocols offer user friendly, well-built secure mechanism that gives confident to the users and healthcare professional to access the e-health system. These protocols are efficient in terms of maintaining strong user privacy. CAAPA provides high communication overhead compared to other protocols.

## Keywords

Mobile agent, Certificate authority, Public Key infrastructure, policy, privacy, audit, safe

## 1. INTRODUCTION

E-health system has been used as communication system that enables to deliver medical service over the Internet. The growth of information technology has made easy electronic health service in a way doctors keep the records of patients in an information system and make decisions promptly after discussions with experts over Internet. Thus, patients can able to get better medical services with the assist of the system. Moreover, the medical information’s available in health system are highly sensitive and distributed that demands strong authentication and authorization mechanisms for communication between the healthcare professionals, consumers and providers. While it is very important that a way to allow the healthcare professionals that include doctors, nurses, administrative staff, support staff and IT staff have access to the specific information about the patient data for the job and also maintain patient privacy and confidentiality issues that expose the healthcare providers and users liability [1].Internet is essential in enabling to organize, share and access to the medical services. It is required to promote secure and efficient medical service communication over Internet. Security controls must be evaluated in terms of its functional benefits for protecting the privacy of the patient and accurate information to service providers and healthcare professionals. The healthcare providers are responsible for defining differentiated access rules which protect the patient data and related information securely. The access rule is assigned to the health professionals based on the latest values in the attributes. The motivation for dynamically assigning the policy is not for security, but simply the desire to prevent legal health professionals from “gaming” the system [3]. Authorization is defined as a process of granting permission to do or not. A large number of techniques may be used to authenticate a user such as passwords, biometric techniques, smart cards, digital signatures and digital certificates [2].

To enable resource sharing between multiple heterogeneous healthcare enterprises securely, this paper introduces three communication protocols namely Certificate based Authentication and Attribute based Policy assigned Authorization (CAAPA) ,Token based Cross Verification (TCV) and Secure and Auditable Agent- based Communication Protocol (SAACP) frameworks for Mobile e-health systems over Internet. CAAPA is based on message passing technique in which the communication overhead is high and TCV is based on Mobile agent in that the communication overhead is less compared to CAAPA. TCV used encryption/decryption, digital signature and hash code are used as protection mechanism for secure communication between healthcare professionals. The computation load of the TCV protocol is balanced at source, destination and intermediate mobile agent which in turn provide effective performance compared to CAAPA. Secure and Auditable Agent based Communication Protocol (SAACP) performs based on key exchange mechanism using mobile agents to reduce the delay in communication. In this framework, mobile agents are encapsulated with different functionality for achieving different assignments. The mobile agents are chosen to carry sensitive information during a communication in e-health system. However, mobile agents are also exposed to security threats, which are threats from malicious hosts and malicious agents [13]. Agent carrying information must be protected against other malicious agents that can tamper with its code or data. To avoid these threats, digital signature, hash table, encryption/decryption protocols are used to protect the mobile agent code and carried message. In this proposed frame work, the above techniques are used to protect the code of the agent and carried message very effectively. These architectures help to provide secure and privacy protection to all users accessing the mobile e-health systems. The rest of the paper is organized as follows: In section 2, outline the related work. The proposed security and personalized framework is presented in section 3.Implementation is described in section 4. The conclusion and future work is discussed in section 5.

## 2. RELATED WORK

Burgsteiner et al. [2, 5] proposed a framework which provides secure communication for mobile e-health applications. With the help of this framework, users securely connected and process medical data according to current legal regulations through a secured communication server acting as a relay between mobile devices and data storage. All communication is secured from one end to the other with strong standard cryptographic algorithms. Xianping Wu et.al [4] proposed a secure authentication and authorization management mechanism for protecting privacy in sensitive information systems using dynamic key based group management. The proposed architecture splits into several administrative areas based on geographical location. Each area has Local Secure Group Controller (LSGC) to manage sensitive information sharing and accessing LSGC consists of Strong Authentication Server (SAS), Key Server (KS), an Access Control Server (ACS) and a Record Tracing Server (RTS) to manage users joining and leaving. KS is based on onetime keys instead of unique key encryption key to enhance security.

Song Han et al. [3] proposed security architecture that will integrate the role-based method and attribute certificate based method for e-health system. It is best suit to the system in terms of identity management. This architecture provides secure, efficient and flexible way of administration in e-health system. The design and implementation of the role and privilege authentication is not discussed in the paper. An authorization and authentication architecture for e-health services system that integrates the role-based method [6] and attributes certificate based method [7] into the electronic health service system is discussed in [8]. A finger print –based model suitable for medical images privacy protection against unauthorized recipient is discussed in [9].

## 3.PROPOSED FRAMEWORK

### *3.1 CAAPA*

This section discusses CAAPA the proposed communication protocol which is based on message passing technique. The purpose of this work is to provide privacy protection for each healthcare professional (HP) that helps to accomplish the service. We assume that each healthcare professional is assigned with a policy that manages the permissions needed to complete the tasks. A policy is automatically assigned by the system based on the attributes of the healthcare professional. Suppose, Healthcare professional wants to access the medical data in the remote domain, the following authentication mechanism is used. First, user must be authenticated to the local e-health system. At the second level, there should be a remote access authentication system. In the proposed framework, each autonomous domain has its own Certificate Authority (CA). We assume CAs are trusted entities. CAs are responsible for the creation, digitally signing and distribution of certificates to users registered in that domain. Initially every user obtains an identity certificate from CA. A certificate is an electronic credit card that establishes the user identifies when accessing the system on the web. It contains the name, a serial number, expiration dates, a copy of the certificate holders public key and the digital signature of the certificate-issuing authority so that recipient can verify that the certificate is real. The practice implemented in the proposed authentication mechanism is shown in Figure-1.

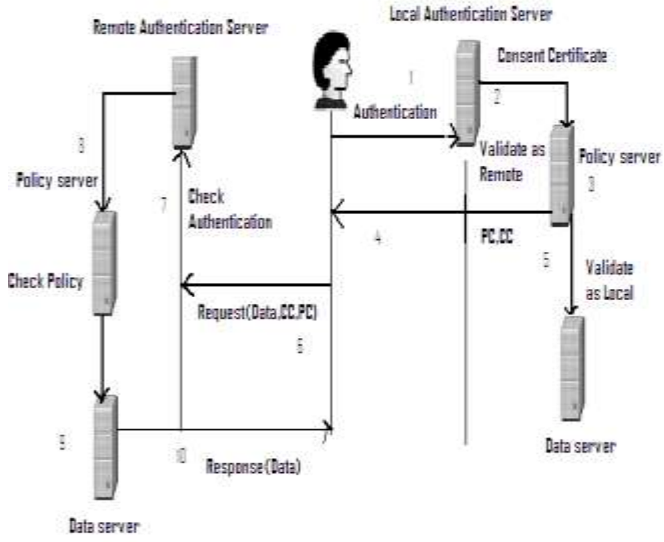

**Figure 1**: Communication of CAAPA

When User begins a new session for remote data request,the local authentication server validates the identity and authenticate by using the certificate and password.The Policy Certificate (PC) is gathered from the Policy Sever(PS) using the valid certificate and attributes of the user for authorization. User request is then forwarded to the remote authentication server for data along with consent certificate (CC) and Policy Certificate (PC). The CC is the authentication that the user has rights to access the medical data in the remote domain.The PC is the policy certificate that manages the permissions needed to complete the tasks When the remote authentication server recieves the access request from the user, it sends the policy certificate to the local server for verification.PC verification is the process of

Mobile agent technologies are used to provide transparent, secure, interoperable, and integrated e-Health information systems for the provision of adapted and personalized sustainable services to the citizens. The purposed of using mobile agent is to reduce cost and to deliver health care services at a distance [10]. Holt et al. proposed hidden credentials [11], a system that protects sensitive credentials and policies. Furthermore, the system reduces the network overhead as it needs fewer rounds of interaction compared to traditional trust negotiation. Fahed Al - Nayadi et.al proposed a dynamic, distributed and heterogeneous policy framework for sharing medical information among autonomous and disparate healthcare information systems in P2P environment [12]. This framework provides privacy, confidential and security to all the healthcare professionals accessing the system establishing an understood level of confidence that an attribue applies to a specific individual.After sucessful verfication, the requested data as response back to the user.Maintaining the challenges of privacy has always been challenge in e-health system. Each certificate binds a username and an attribute. Each user in the system has a unique username and attribute associated with the certificate. The policy assigned to the health professional dynamically to provide privacy protection for both access control policy and certificate.

Let S be a set of defined policy functions i.e., S= {$P_1$, $P_2$…..Pn}.Each user belongs to any of the policy in S depends on its attributes. A policy function in S is chosen based on the attributes values {attr1, attr2….attr n}.An attribute is a statement about a certificate holder. For example, an attribute be gender (male or female), age (between[0-17],between[18-20],between[21-59] or age>=60),annual income(between[0-15k],between[15k-30k],income>60K),category(Government, Private, Owner),label (Professor, Politician,Technican, Accountant, Officer, attender), Grade(A,B,C,D), disease type(S,P,N). Each user in the system has a unique name and an attribute attr. A policy in set S is dynamically assigned for the user based on the latest values of user attributes. The following statements clarify the above statement. Let $C_A$ be the certificate of user A, to check whether A satisfies any policy in the Set S if S ($P_i$) =1.Suppose that x patient attribute is Male^60^private^accountant^D^P.In policy set, the attribute matches with at least one policy that is assigned to the patient. Suppose, the attribute satisfied with many policies, the highest one is assigned to that patient.

For better privacy, the attribute is protected using encryption. If the attribute M1 >M2 then E (M1)>E (M2). Table-1 and Table -2 shows the original and encrypted data for age.That is to say the structure of original data is same to the structure of secret data. The algorithm for encryption is as follows

*(1)Make original data m transformation:*

$$c' = E'(M) = a_0 m^3 + b_0, \quad a_0, b_0 \ € \ Z$$

(2) Make c' encryption transformation:

$$c = E(c') = (c' + e*p) \bmod (p*q) \quad p,q \ € \text{ prime }, \ e \ € \ Z.$$

**Decryption:**

(1)Make c decryption transformation D(c)=c mod p, get c'.

(2) Make c' adverse transformation, then original data.

### 3.2 TCV

TCV is another secure protocol proposed to reduce the communication overhead by using Mobile agent. Mobile agent is defined as a program that can migrate or move from a home platform to another, carrying its code and data. When migrating, the agent invokes a method for migration. Once migrated, the code will be executed in the remote platform and the original agent is destroyed. The remote platform is responsible to create the agent and allow it to execute once it arrive there. At the remote platform, the mobile agents may communicate with the agents may communicate with the agent in the remote platform to negotiate and ask for resources. TCV describes the communication protocols between two parties Doctor and Patient, which involve a mobile agent. Doctor agent creates an instance of a mobile agent and dispatches to the patient's host, carrying the encrypted plain text. The mobile agent is executed at the patient's host environment. The mobile agent communicates with the patient agent in the process to discover the plaintext. The communication protocol between Doctor Agent (DA), Patient Agent (PA) and Mobile Agent (MA) are described in the next paragraph.

Initially, DA prepares the plaintext and applies security mechanism to protect the plaintext and MA code. DA sends a request to PA to send a message.PA ensure the trust of DA. It is satisfied then it send "Accept "message to DA through MA and DA creates the instance of MA and dispatches it to carry the data to PA's host. PA does not satisfy with DA, it sends the "Reject "message and communication between DA and PA is disconnected.

MA arrived at PA and requests PA to process the carried data. PA process the data and inform the code is valid or not to be executed. If the code is valid, MA gives the token and requests PA to sign in it. Once signed, MA sends the token back to the DA. DA validates the token and gives the encrypted information to MA. MA decrypts, recover the plaintext and applied hash function on the plain text. PA verifies the hash function, process the data and return to MA. MA informs the results to DA and terminates.

In this protocol, the following security measurements are considered and verified among DA, PA and MA. The protection of plain text is to avoid unauthorized access or modification from any third party. This is done by using symmetric key (Sk). Hash function is applied to ensure that plaintext is unmodified .Token is used by the DA through MA to ensure the identification of PA, MA collects the Sk from DA for decrypting the plain text. The validity of MA code is also checked by the PA before the transfer of data between PA and DA.

## 3.2 SAACP

This section discusses the proposed secure communication protocol SAACP between doctor and patient. Doctor wants to analysis the patient information which is available at remote site. The proposed secure communication protocol framework is shown in Figure -2.

Each domain consists of Certificate authority server, Policy server and data server. Certificate authority server is a trusted third party in charge of acknowledging the validity of public keys or other secrets used for authentication. It is also responsible for providing the necessary information for authentication between the trading parties throughout the transaction.

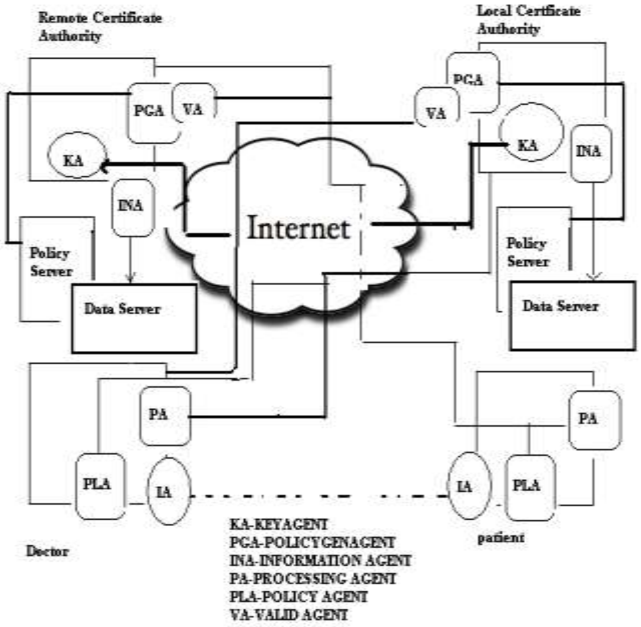

**Figure 2**: Framework of SAACP

This server identifies the proof of identity of the user. Policy server generates the policy based on the attributes of the user in the data server. Data server keeps the medical data and attributes of the healthcare professionals and patients. The term *policy* is defined as a set of permission given to the specific user for accessing the level of information. Generally, policy is assigned statically whereas in this protocol, it is assigned based on the latest attribute values of the user. A set of policy is defined .Any one policy is chosen from the set based on the latest values of the user. The policy of the user is generated at both sites and verified the consistent. In this frame work, mobile agent is encapsulated with different functionalities and assigns to perform some distinguished assignments. There are six different functionalities mobile agents are proposed and used in this frame work.

**KEY AGENT**: Each Certificate Authority (CA) offers with one KEYAGENT. KEYAGENT dispatch to remote CA for getting the public key of the specific healthcare professionals registered under it. This agent activates by the CA if and only the specific healthcare professional is not a member of the CA.

**PROCESSING AGENT**: After receiving the public key of the recipient, Sender initiates the request by using PROCESSING AGENT to the remote CA.PROCESSING AGENT helps to create a secure communication between the parties.

**POLICY AGENT**: After receiving the *accept* message from the recipient. Sender dispatches the POLICY AGENT to the remote CA for the level of permission to access the medical data. Policy certificate is cross verified with the help of local policy server.

**INFOPOLICY AGENT**: Remote CA initiates the INFOPOLICY AGENT after sending the Public key requested by the sender. INFOPOLICY AGENT collects the latest attribute values of the sender for generating the policy certificate.

**POLICYGEN AGENT:** The INFOPOLICY AGENT value is copied into POLICY AGENT. It carries the information to the policy server for generating the certificate.

**VALID AGENT**: The policy certificates from the POLICY AGENT and POLICYGEN AGENT differs, the retransmission of another POLICY AGENT from the sender is informed through VALID AGENT. It is only initiated there is a difference in the policy.

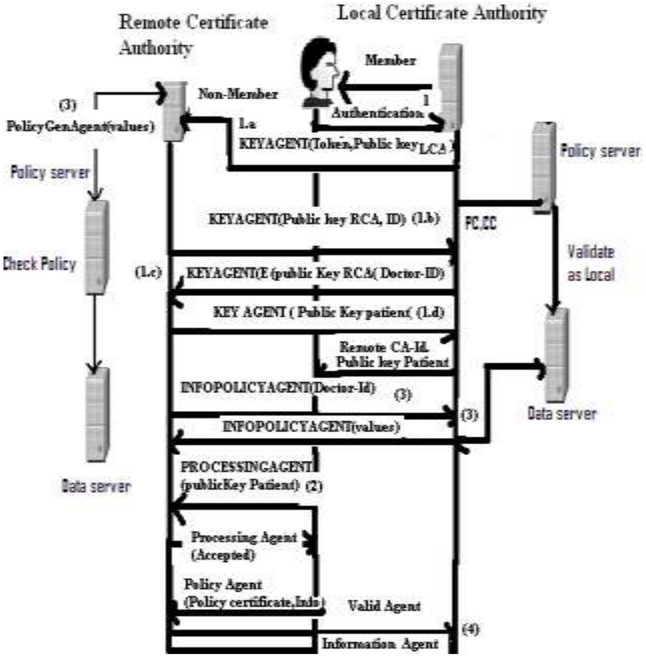

**Figure 3:** SAACP communication protocol

SAACP protocol communication between doctor and patient at remote site is shown in figure 3.The detail communication between doctor and patient at remote site based on SAACP is given as below.

Step1: Doctor requests the public key $_{\text{patient}}$ from the local Certificate Authority (CA).

(1.a) Patient is not a member of CA, KEYAGENT dispatch to the remote CA along with Token, Public Key $_{\text{LCA}}$. Patient is member of CA then the public key $_{\text{patient}}$ issue to the Doctor.

(1.b) KEYAGENT arrived at the remote CA. Remote CA checks the code of KEYAGENT is valid or not. If it is valid, KEYAGENT gives the Token to Remote CA and requests to sign in it. Remote CA gives the Public Key $_{RCA}$ , Remote CA-ID to the KEYAGENT after encrypt using Public Key $_{LCA.}$

(1.c) KEYAGENT back to the Local CA. Local CA validates the Token. After satisfied, decrypt the Public Key $_{RCA}$ and dispatches the KEYAGENT along with the E $_{\text{public key RCA}}$ (Doctor-Id).

(1.d) Remote CA decrypts the Doctor-ID and provides the Public key $_{\text{patient}}$ back to the Local CA. Local CA returns the same to the Doctor along with Remote CA-ID. Meantime, Local CA collects the values of the doctor from the Data Server using INFOPOLICY AGENT.

Step 2: Doctor dispatch the PROCESSING AGENT to the Remote CA-ID with the copy of Public key $_{\text{patient}}$ .After validates the code of PROCESSING AGENT , the Remote CA sends the “accept “ message back to the Doctor . Otherwise, the communication is disconnected.

Step 3: Doctor transmit the POLICY AGENT along with the required informationto the Remote CA and policy certificate. Remote CA checks the policy of the doctor with the generated policy using by the Local Policy Server with the help of POLICYGENAGENT. After the verification, the required information is encrypted using Public Key $_{LCA}$ and sends to the doctor by INFORMATION AGENT. It decrypt at the receiving side by the private Key $_{\text{Doctor}}$.

Step 4. Policy is mismatched with the generated one. Trust of the POLICY AGENT is questioned, remote CA request the doctor by using VALID AGENT to retransmit the POLICY AGENT again.

## 4 SIMULATIONS

The proposed framework is implemented as prototype in JAVA. User has being accessed the framework through mobile, laptop and desktop. Mobile device is used to send and receive the information as SMS from the framework. User can get all types of information such as doctor list, patient details, status of patient etc through Web. The messages from public users are also processed in this health care system after some verification. If the message indicates about the accident, based on the human organ damaged, the health system filters the specialists and identifies the nearby doctor available and directs the ambulance to go to the accident spot, then specifies the nearest doctor’s availability and makes the ambulance to go to that nearest hospital immediately. The following operation in Figure -3 is performed when the message is from the private user. The server retrieves the name of the doctor from the doctors profile database. If the message from the private user specifies that the doctor is entering into the hospital, then the server updates the doctor with the public user message, particular password status as ‘IN’ in the available doctors Database, so that when the private message service identifies the availability of the doctor in the nearby location. If the message from the private user specifies that the doctor is leaving the hospital, then the server updates the doctor with particular password status as ‘OUT’ in the Available doctors Database, so that when the private message service provide filters the n on available doctors from the process of allocation.

The operation shown in Figure -4 is performed when the message from non-registered user. First the server identifies whether the incoming message is for requesting appointment from doctors or conveying about the accident. If the message is for fixing appointment, then the public service message provider identifies the availability of doctor and the timing is assigned for the patient and the reply to the public user immediately and makes an entry in the appointment database too. The appointment database deletes all the records once in every 24hrs.

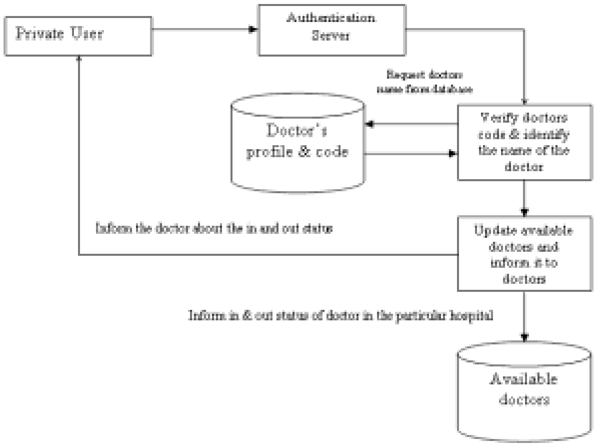
Private User
Authentication Server
Request doctors name from database
Doctor's profile & code
Verify doctors code & identify the name of the doctor
Inform the doctor about the in and out status
Update available doctors and inform it to doctors
Inform in & out status of doctor in the particular hospital
Available doctors

**Figure 4**: Private User Message processing

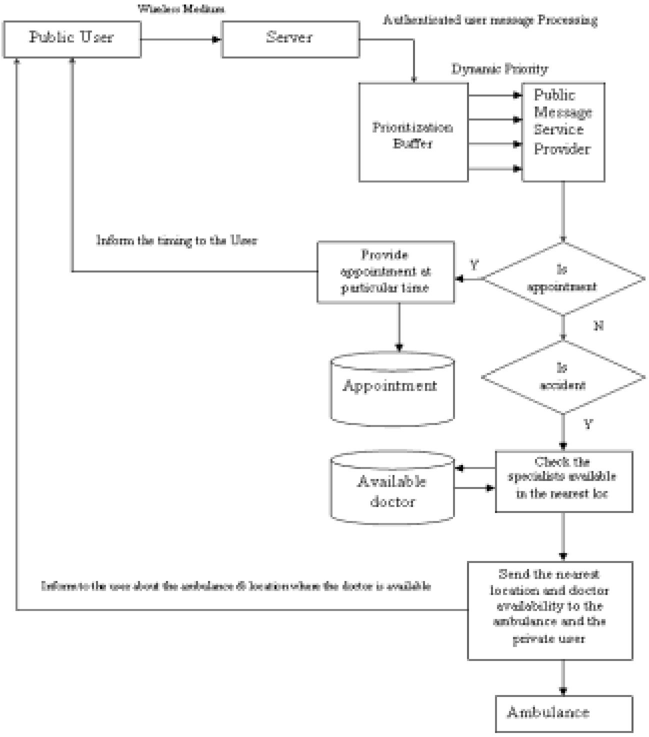
Wireless Medium
Public User
Server
Authenticated user message Processing
Dynamic Priority
Prioritization Buffer
Public Message Service Provider
Inform the timing to the User
Provide appointment at particular time
Y
Is appointment
N
Appointment
Is accident
Y
Available doctor
Check the specialists available in the nearest loc
Inform to the user about the ambulance & location where the doctor is available
Send the nearest location and doctor availability to the ambulance and the private user
Ambulance

**Figure 5**: Functionality carried by the system when the request from non-registered user

## 5. CONCLUSION

In this paper, three secure communication protocols for E-health system are proposed. These protocols provide secure and flexible communication between user and healthcare system. The proposed system offers a number of advantages including a user-friendly, strong authentication and gives confidence that systems are secure. The limitation of this system is the user should specify the location where the accident happened. Hence, the proposed approach will be extended with the help of Global Positioning System (GPS) to track the location and utilize the transport facility of the organization very effectively. Medical data are stored in encrypted format and send to the legitimate user.

## 6. REFERENCES

[1] Alessandara Toninelli, Rebecca Montanari and Antonio Corradi," EnablingSecure Service Discovery in Mobile Healthcare Enterprise Networks",IEEE wireless Communications June 2009 pp.24-32.

[2] Blobel B, Advanced and Secure Architectural HER Approaches,(Int.Journal Medical Informatics, 2006), pp- 185-190.

[3] Burgsteiner H and Prietl J, A Framework for secure communication of Mobile E-health applications", in *Medical Informatics meets eHealth* (2008) pp.29-30

[4]Burgsteiner Harald, Wallner Dietmar,"PeDIS-Design and Development of a Performance Diagnosis Information System", ( Medical Informatics meets eHealth ,2008), pp. 47-51.

[5] Fahed Al-Nayadi, Jemal H.Abawajy, An authentication Framework for e-health systems", *in Proc. Int. symp. Signal Processing and Information Technology (IEEE, 2007)*, pp., 616-619.

[6] Fahed Al-Nayadi and J.H.Abawajy, An Authorization Policy Management Framework for Dynamic Medical Data Sharing in *Proc. Int.conf. Intelligent Pervasive Computing (IEEE, 2007),* pp.313-318

[7] Han, Song and Skinner, G. and Potdar, Vidysagar and Chang, Elizabeth and Wu, Chen, New Framework for Authentication and Authorization for e-Health Service Systems, in *Proc.Int. Conf.Industrial Technology* (2006), pp. 2833-2838.

[8] Hitchens M, Varadharajan V, Design and Specification of Role-based Access Control policies. in *IEE Proc. Software* (2000), pp.117-129.

[9].J.E.Holt, R.W.Bardshaw, K.E.Seamons, and H.Orman, Hidden credentials, *in Proc. second ACM workshop Electronic Soc* (2003), pp.1-8,2003.

[10] Li M, Poovendran R, Narayanan S, Protecting Patient Privacy against Unauthorized Release of Medical Images in a Group Communication Environment, (Int.Journal. Computerized Medical Imaging and Graphics,2005),pp. 367-383.

[11]Panagiotis Germanakos1, Constantinos Mourlas1, and George Samaras2, A Mobile Agent Approach for Ubiquitous and Personalized eHealth Information Systems, ( IEEE transactions on computers ,2006) pp.1259-1273.

[12]Rossilawati Sulaiman, Xu Huang, Dharmendra Sharma,"E-health services with Secure Agent",in proc.7th Annual communication Networks and Services Research Conference 2009, pp. 270-277.