Secure and auditable agent-based communication protocol for e-health system framework

M. ARAMUDHAN[1] and K. MOHAN[2]

[1]Perunthalaivar Kamarajar Institute of Engineering and Technology, Nedungadu, Karaikal (India).
[2]School of Computational Science & Engineering, VIT University, Vellore - 632 014 (India).

(Received: October 21, 2010; Accepted: November 19, 2010)

ABSTRACT

Security is essential for e-health system as it provides highly sensitive distributed medical data and exchanged among the healthcare professionals, customers and providers over Internet. Internet is an open access system that allows anyone to participate and access the data. Hence, it is necessary to protect the data, service from the unauthorized visibility, use and also maintain a high degree of accessibility. It is achieved using suitable access control policies and techniques that enforce differentiated levels of service visibility and access to the users. This paper introduces a Secure and Auditable Agent- based Communication Protocol (SAACP) which performs on key exchange mechanism with mobile agents to reduce the delay in communication. Intelligent mobile agents are proposed for dynamically negotiating the policy of the users. This protocol offers user friendly, privacy and safe communication through well-built secure mechanism that gives confident to the users and healthcare professional to access the e-health system.

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

INTRODUCTION

E-health system has been used as communication system that enables to deliver medical service over the Internet. Internet is an open access system that allows anyone to participate and access the data. The growth of Internet and information technology has made unproblematic electronic health service that offers a scheme for the doctors to 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, improves their relationship and provides online education through online resources. Moreover, e-health system provides highly sensitive distributed data that demands strong authentication and authorization mechanisms for communication between the healthcare professionals, consumers and providers. While it is very important the manner in which the healthcare professionals that include doctors, nurses, administrative staff, support staff and IT staff are allowed for accessing the specific information in the medical data for their service and also sustain the issues such as privacy and confidentiality[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 consumers, 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. In the existing access control mechanism, the granting of access rights requires statically binding a subject (doctor) to a target (patient data), where subject and target is known in advance. A better solution is to define the access rights in more general term. 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].

Mobile agent is defined as a specific form of mobile code that can transport from one environment to another, with its data intact, and be capable of performing appropriately in the new environment. To enable resource sharing between multiple heterogeneous healthcare enterprises securely, this paper introduces a communication protocol called Secure and Auditable Agent based Communication Protocol (SAACP) which performs on key exchange mechanism with 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. The rest of the paper is organized as follows: Section 2 discusses the related work. SAACP architecture is discussed in section 3. The implementation is explained in section 4 and this paper is concluded with a summary in section 5.

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. Xian ping 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.Rossilawathi Sulaiman *et al.,*[14] proposed a secure communication protocol based on mobile agent. In this protocol, agent itself carries the protection mechanisms without depending on the senders/owners platform. At the destination side, the mobile agent code is authenticated and the code requests a service from the platform to decrypt the message. To avoid the malicious code injection to the data carried by the agent, the mobile agent carries its own protection by using disposable key pair.

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].

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

Proposed Framework

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 -1.

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. 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.

SAACP protocol communication between doctor and patient at remote site is shown in figure 2.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)

a) Patient is not a member of CA, KEYAGENT

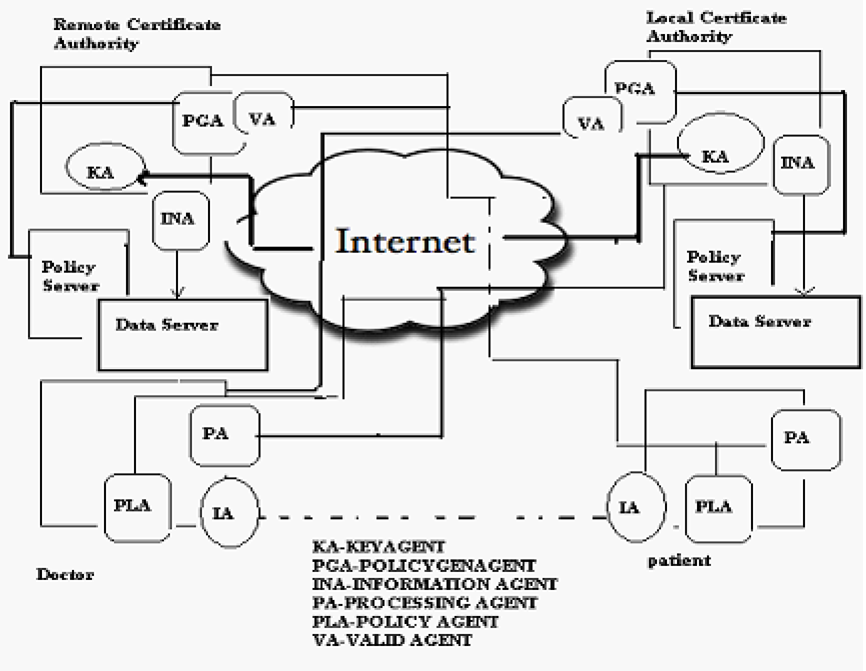

Fig. 1: Framework of SAACP

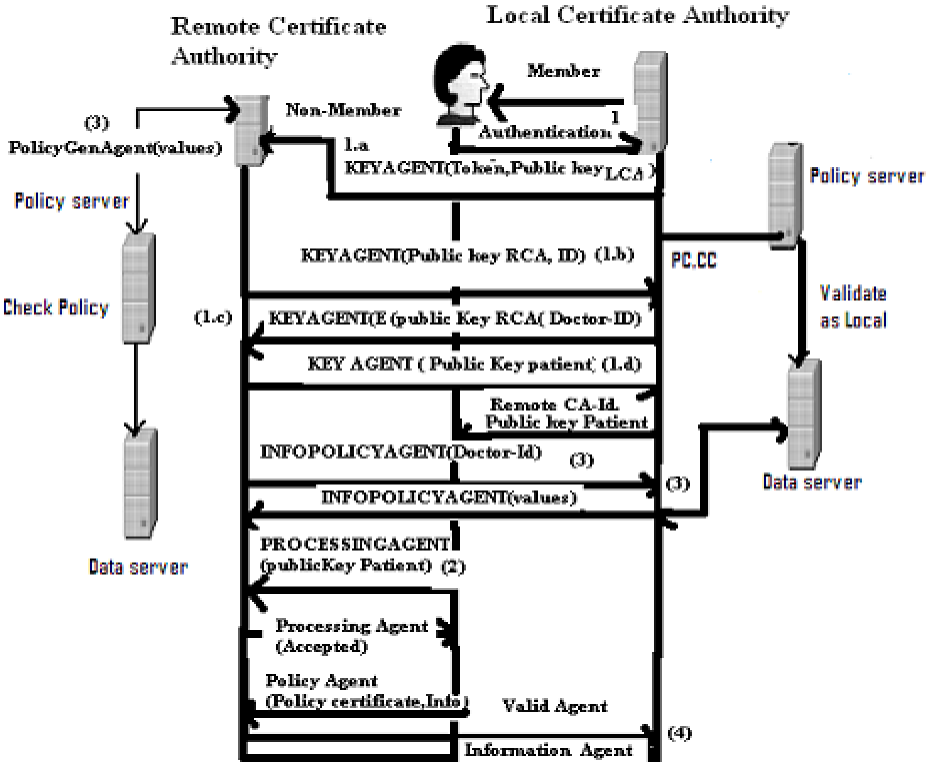

Fig. 2: SAACP communication protocol

dispatch to the remote CA along with Token, Public Key $_{LCA}$. Patient is member of CA then the public key $_{patient}$ issue to the Doctor.

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 $_{LCA.}$

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 $_{public\ key\ RCA}$ (Doctor-Id).

d) Remote CA decrypts the Doctor-ID and provides the Public key $_{patient}$ 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 patient

After validates the code of PROCESSING

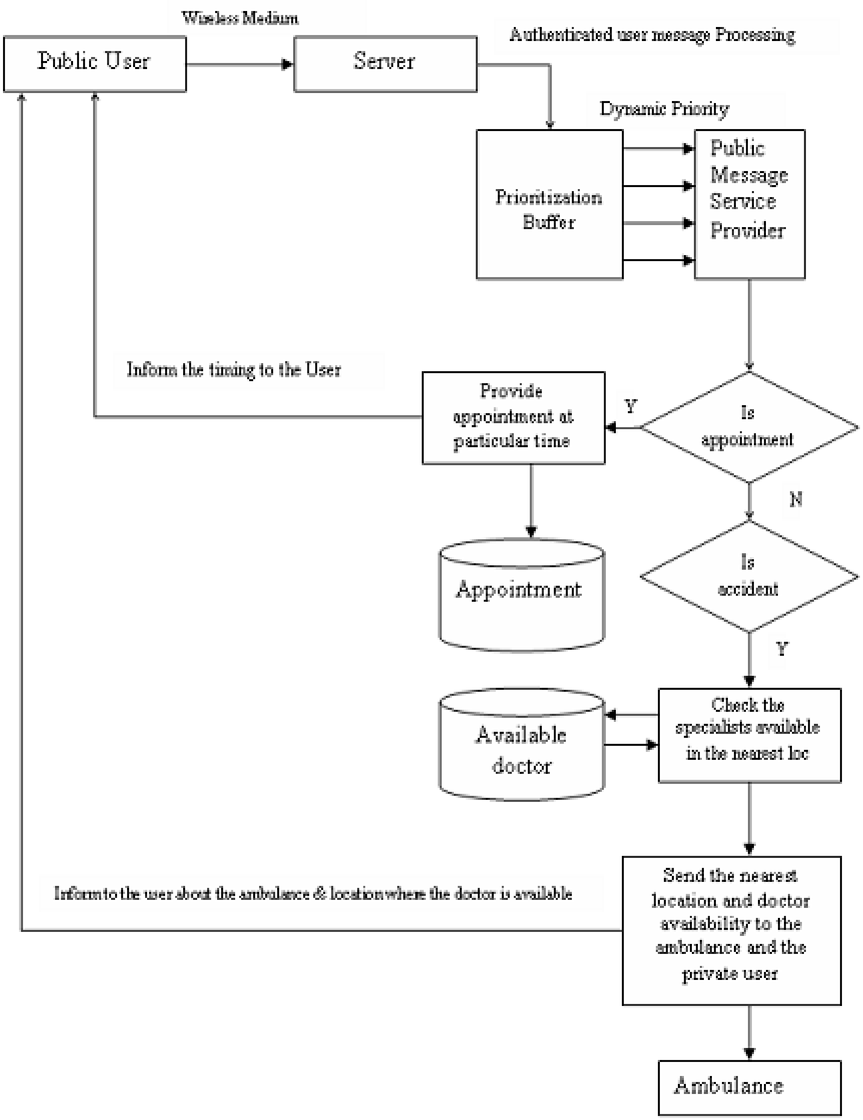
Wireless Medium
Public User
Server
Authenticated user message Processing
Dynamic Priority
Prioritization Buffer
Public Message Service Provider
Inform the timing to the User
Provide appointment at particular time
Y
Is appointment
N
Appointment
Is accident
Y
Available doctor
Check the specialists available 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

Fig. 3: Functionality carried by the system when the request from non-registered user

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 $_{Doctor}$.

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.

Simulation

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.

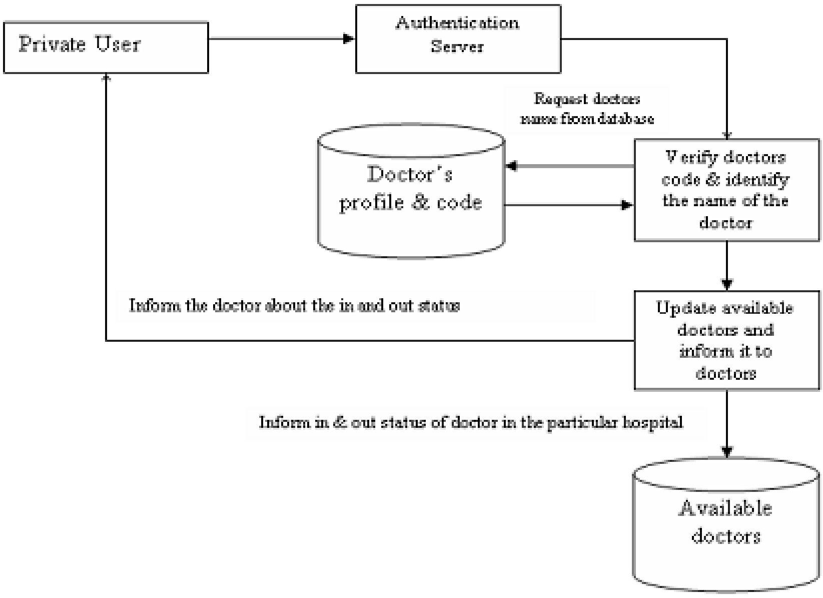
Private User
Authentication Server
Request doctors name from database
Doctor's profile & code
Verify doctors code & identify the name of the doctor
Inform the doctor about the in and out status
Update available doctors and inform it to doctors
Inform in & out status of doctor in the particular hospital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

Fig. 4: Private User Message processing

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.

CONCLUSION

Future Work

In this paper, a new secure communication protocol SAACP is proposed for E-health system framework. This protocol provides 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 transmitted in encrypted format and send to the legitimate user after various levels of verification. In this protocol, six different mobile agents with different functionalities are proposed and used very effectively for the benefits of secure communication.

REFERENCES

1. 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.
2. Burgsteiner H and Prietl J, A Framework for secure communication of Mobile E-health applications", in *Medical Informatics meets eHealth* 29-30 (2008).
3. Song Han, Geoff Skinner, Vidyasagar Potdar, Elizabeth Chang,A Framework of Authentication and Authorization for e-Health Services *in Proc. SWS* 105-106 (2006).
4. Xianping Wu, Huy Hoang Ngo, PhuDungle,balasubramaniam srinivasanii, Novel Authentication & Authorization Management for Sensitive information Privacy protection using Dynamic Key based Group Key Management", (Int. Journal of Computer Science and Applications, 57- 74 (2009).
5. Burgsteiner Harald, Wallner Dietmar,"PeDIS-Design and Development of a Performance Diagnosis Information System", (Medical Informatics meetse Health) 47-51 (2008).
6. Hitchens M, Varadharajan V, Design and Specification of Role-based Access Control policies. in *IEE Proc. Software* 117-129 (2000).
7. Blobel B, Advanced and Secure Architectural HER Approaches,(Int.Journal Medical Informatics) 185-190 (2006).
8. 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* 2833-2838 (2006).
9. 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) 367-383 (2005).
10. Panagiotis Germanakos1, Constantinos Mourlas1, and George Samaras2, A Mobile Agent Approach for Ubiquitous and Personalized eHealth Information Systems, (IEEE transactions on computers 1259-1273 (2006).
11. J.E.Holt, R.W.Bardshaw, K.E.Seamons, and H.Orman, Hidden credentials, *in Proc. second ACM workshop Electronic Soc* 1-8 (2003)
12. 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)* 313-318 (2007).

13. Alessandara Toninelli, Rebecca Montanari and Antonio Corradi," EnablingSecure Service Discovery in Mobile Healthcare Enterprise Networks",*IEEE wireless Communications*. 24-32 (2009).

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