Proposed Secure Protocol for Online Health System in Cellular Communication

M. Sadiq Ali Khan* and Hussain Saleem

Department of Computer Science, University of Karachi, Pakistan

Abstract: Health Services are being offered over the internet by using an online health system. The information available in a system are extremely susceptible and distributed that needs powerful verification and endorsement means for message passing between the experts, clients and suppliers. Nowadays internet is everywhere and everybody is linked with this internet community and accessing the world with their finger tips. Hence, online users require secure communication and consumer confidentiality over the Internet. We bring protected communication protocols for online e-health system. Certificate based Authentication and Policy assigned Authorization mechanism for a Cellular health system is proposed. We proposed a set of rules for online health system based on cellular agent. This set of rules provides strong security to users and experts in that domain. Our design is capable in keeping the confidentiality of the user.

Key Words: authorization, authentication, access control, certificate, information technology.

1. INTRODUCTION

By the help of an online health communication system medical services can be delivered across the world through internet technology. The rapid growth of IT provides easiness to physicians in maintaining the patient database and made conclusions after negotiating with the filed experts over the system. Thus, better medical services are delivered through this system. Furthermore, the medical info available in health management system is extremely susceptible and disseminated that demands well-built communication security mechanism for authentication and authorization between the experts and customer. It is a great matter of concern that how we permit the experts consists of physician, managerial staff, technical staff and clerks have access to the explicit info regarding the patient record for the career and in addition preserves patient confidentiality and privacy problems that infer the providers and consumer users liability [1]. In today's world where technology facilitates users more efficiently and promptly, internet is also helping people regarding their medical issues. We need secure communication over Internet. Security measures should be evaluated in terms of its functional benefits for preserving the secrecy of consumers and provide precise info to experts. The providers are responsible for defining differentiated access rules which protect the user data and related information securely. The rule for accessing the data is assigned based on the current values in the attributes. The incentive for dynamically assigning the policy is not for security, but simply the desire to prevent legal health professionals [3]. Authorization is defined as a process of yielding consent to carry out or not, to check whether the person accessing is legal or not [6]. Numerous methods may be used to authenticate a user like passwords, biometric techniques and digital certificates etc. [2]. To facilitate peoples we introduce message passing rules for cellular online health systems over the Internet. CBAPAM is based on communication techniques having more overhead and Token mechanism which is based on cellular agent having smaller amount of overhead. It used cryptographic techniques and hash algorithms. The working load of the Token based protocol is fair at user side, target and midway cellular agent which offer helpful performance in contrast with others. These systems assist in providing security protection to consumer accessing the cellular online health systems. In next section literature overview is discussed, then security methods is proposed, in the end modeling and conclusion talk about.

2. LITERATURE SURVEY

In [2 & 5] structure was proposed for mobile online health applications. Due to this, users firmly associated and process health records using a secured communication relay. All over communication is protected from one end to the other with sets of cryptographic techniques. Secure verification techniques and management of user authentication methods for preserving the systems was proposed in [6] explained in [3]. The architecture for online health system, which offers secure, well-organized and supple way of management in online health system. An architecture for online health services system that put together methods proposed in [4 and 7] into the electronic health service system is discussed in [8]. An identity based model appropriate for health system images secrecy against malicious user is discussed in [9]. Tools for agent based are used to provide safe and integrated online health information systems, in order to reduce the expense and to provide services at a distance [10]. A scattered and mixed policy

*Address correspondence to this author at the Department of Computer Science, University of Karachi, Pakistan; E-mail: msakhan@uok.edu.pk

0250-5363/08 © 2008 University of Karachi

structure for sharing health info in P2P atmosphere is proposed in [11]. This structure provides secrecy and protection to all the experts of the systems.

3. PROPOSED STRUCTURE

3.1. CBAPAM

CBAPAM, is based on message passing and provides secrecy protection for experts that helps to carry out the services. Each individual can access the system with the help of approved policy infrastructure. System assigned the policies by itself keeping in view the value of the user. If someone wants to access the records in the distant domain, according to rules initially user must be authenticated to the confined online health system then there should be a distant access authentication system. Every domain has its own CA which is faithful unit. A certificate contains the identification, a index number, ending dates, public key copy and the digital signature of the authority who issued the certificate so that consumer can endorse it. The proposed verification method described below in Fig. (**1**).

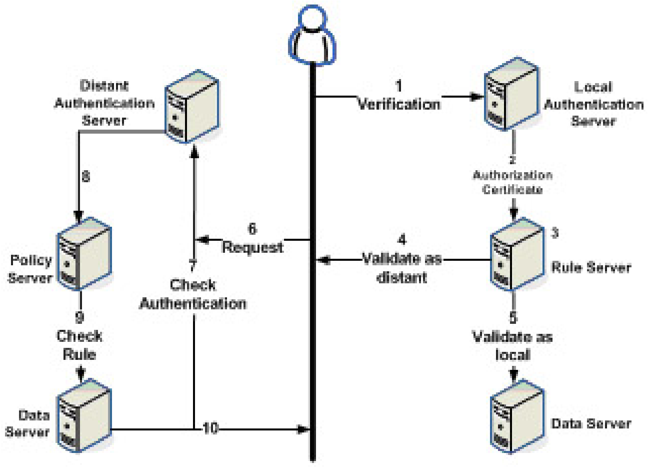

Fig. (1). Communication of CBAPAM.

When user starts in requesting the distant record, the local server authenticate then identity by using the certificate and code word. The Rule Certificate (RC) is gathered from the Server which mantains the policy by using the certifcate and its attributes. It then forwarded to distant authentication server for record along with authorization certificate (AC) and rule certificate (RC). All the permissions needs to fulfil the task managed by the RC when server receive the valid request from the user side, it sends the RC to server for authentication. Every certificate attaches a consumer id with its attribute value. User assigned a policy in order to provide secrecy protection for both policies (access measures, certificate).

For example P_m act as policy functions comprises of different policies. Each consumer associated with any one of the policy depending on its feature. A policy function is selected based on the feature standards. A feature is a declaration about a certificate owner. e.g. a feature be sex, age, annual income ({0 to 10000}, {10,000 to 25000}, {25000 to 60,000}, {greater than 60,000}), category (G, P, O), tag (Educationist, Politician, Technician, Accountant, Attendant), Grade (I, II, III, IV), illness category. A policy is allocated for the user based on the current values of user features. Let Cu be the certificate to make sure whether user assure any regulation in the policy set. In policy set, the feature matches with at least one policy that is allocated to the patient. If feature fulfilled by different policies, the top one is allocated to that user. Encryption is applied to protect the features as mentioned below Formulate real message / record *m* alteration:

$$C' = Enc'(M) = x_0 m^3 + y_0; x_0, y_0 \in Z$$

Formulate C' alteration as

$$C = Enc(C') = (C' + e * p)\mathrm{mod}(p * q)$$

Where *p* and *q* are two large prime numbers.

Decryption:

For decryption

$Dcrp(C) = C \bmod p;$ get C'.

3.2. Token Based Secure Protocol

It proposed in order to cut down the overhead by using Cellular user. Cellular user is one which has its code id and data, can move from one platform to another. When transferring occurs the identification carry out in the distant platform. The distant platform allowing cellular users to execute and may talk to other user on distant location. Token based secure protocol depicts the message passing protocols among physician and cellular user. The cellular user corresponds with the patient to find out the actual data. The message passing protocol between Physician User (PU), Patient Agent (PA) and Cellular User (CU) are mentioned as: Initially, PU protect the message by using encryption. PU initiates a query for PA for sending a message. PA makes sure the confidence of PU. By sending “Agreed Upon” message to PU through CU it satisfies and PU generates the instance of CU and transfers it to carry the data to PA’s host. When it does not satisfy with PU, it initiates the “Reject” message and all transmission is cut off. When CU reaches PA it tells PA to process record. If the system id is legal, CU provide the token and requests PA to get into it. Once signed, CU send the token back to PU, it permits the token sends encrypted text to CU. By applying decryption techniques CU recover the message and applied hash function like MD5 on the actual message. PA verifies the MD5 value, process the data and return to CU. CU notifies the results to PU and discontinue.

The security of message is to keep away from any malicious activity from the intruder. This is done by using private key algorithms. Authentication function (MD5) is applied to make sure that original message should be unaffected. Token is used by the PU through CU to guarantee the recognition of PA, CU bring up the key from PU for decrypting the message. The authority of code is also confirmed by the PA before the transfer of data between PA and PU.

4. PROPOSED MODEL

The implementation of our proposed mechanism is possible as prototype in any platform. User can retrieve the structure by means of cell phone, PDA's and PC. User sends and receive the data by the help of cell phone and be able to accept the info from the structure in the form of SMS. User is capable enough to get all kinds of related records though internet by using the system. Unrestricted users messages are also the messages from public users are also processed by this system need some authentication. If specified message shows some injury, the proposed systems filters the consultants and identifies the close by physician availability and tells the emergency medical service to go and bring the injured person, then identify the nearest physician's accessibility and instruct them to reach the adjacent emergency centre instantly. As in the case of private user the operation performed as the server get back the id of the physician and if physician is entering into the emergency centre than the server updates with the message detail, status as 'ENTER' in the accessible physicians records, so that when it pointing out the availability of the physician at the nearest location. If message shows that the physician is exiting from the emergency centre then updates status as 'EXIT' in the available physicians record, in order to filter the unavailable physicians from the method of allocation.

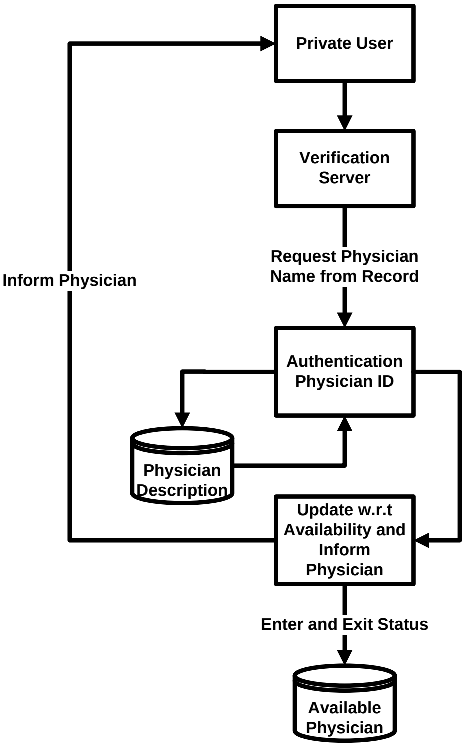

Fig. (2). Private User Message processing.

The Fig. (**3**) shows the process when message is from the unauthorized user. First of all server ensures whether the message corresponds to the appointment of physician or it is the indication of the injury. In case of appointment signal unrestricted message provider recognizes the accessibility of physician and the appointment slot is assigned for the patient and gets back a reply to unrestricted user at once and update the appointment list too. After every 48 hrs entries from the appointment records deleted at once.

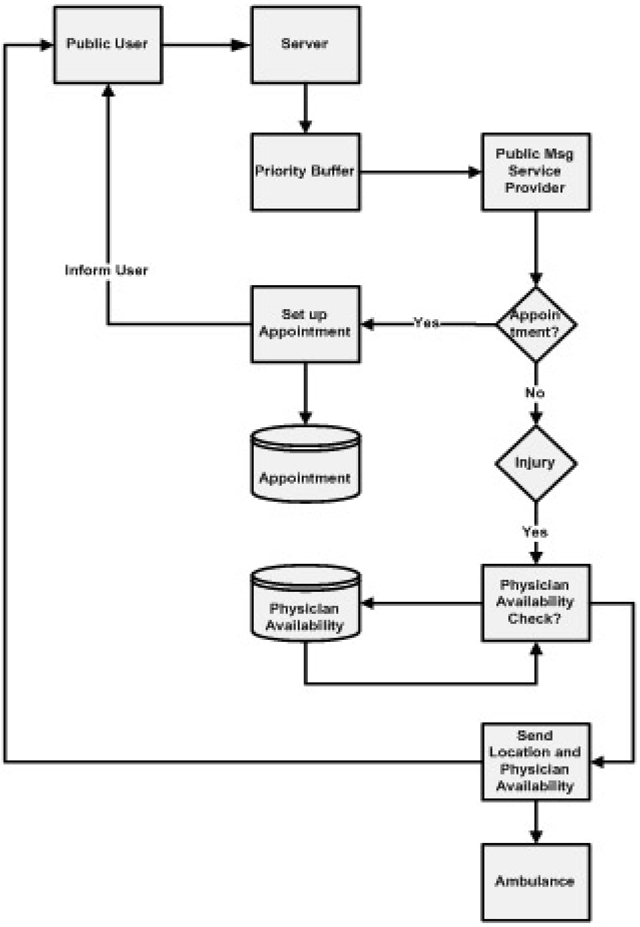

Fig. (3). Elaborate the system tasks in case of unregistered users.

5. CONCLUSION

We proposed secure message passing protocols for online health communication system. This secure set of rules guarantees you to protect communication between consumer and the management structure. It has strong authentication mechanism and provides high degree of confidentiality. It provides good health services over the latest internet technology. We may extend this work by incorporating the automatic location finding scheme to identify the position of the user in order to utilize this system more effectively.

REFERENCES

[1] Brain Randell & et.al (2007), “A computer scientist's reactions to National Program for IT”, Journal of Information Technology 22, pp. 222–234.

[2] Burgsteiner H and Prietl J(2008), “A Framework for secure communication of Mobile e-health applications”, Medical Informatics meets eHealth, pp..29-30.

[3] Snezana Sucorovic & et.al (2007), “Implementing security in a distributed web-based EHCR”, International Journal of Medical informatics”, Vol 76 Issue 5, pp.491-496.

[4] Song Han & et.al (2006), “A Framework of Authentication and Authorization for e-Health Services”, in Proc. SWS , pp.105-106.

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

[6] M.Sadiq Ali Khan & Dr.S.M.Aqil Burney (2005), “Algorithms for Data Security in Wireless Networks”, Karachi University Journal of Science Vol 33(1 & 2) July-December, pp. 53-56.

[7] Gail Joon Ahn(2004), “Role-Based Privilege Management Using Attribute Certificates and Delegation”, Lecture Notes in Computer Science, Volume 3184, pp.100-109.

[8] G. Kambouraki & et.al (2005), “PKI-based secure mobile access to electronic health services and data”, Technology & Health care Journal, IOS Press, Vol 13, pp.511-526.

[9] Dickson K.W.Chiu et.al (2007),” Protecting the Exchange of Medical Images in Healthcare Process Integration with Web Services”, IEEE computer Society, ISBN: 0-7695-2755-8

[10] Panagiotis Germanakos1 & et.al(2006), “A Mobile Agent Approach for Ubiquitous and Personalized eHealth Information Systems”, IEEE transactions on computers , pp.1259-1273.

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