A Secured Model for Indian E-Health System

Shilpa Srivastava[1], Namrata Agarwal[2], Millie Pant[3], Ajith Abraham[4]

[1]RKGIT, MCA Department, Ghaziabad, India
shri.shilpa03@rediffmail.com
[2]NIFM, Faridabad, India
nagrawal@nifm.ac.in
[3]Indian Institute of Technology – Roorkee, India
millidma@gmail.com
[4]Machine Intelligence Research Labs (MIR Labs), USA
[5]IT4Innovations, VSB- Technical University of Ostrava, Czech Republic
ajith.abraham@ieee.org

***Abstract*—**The inclusion of information technology in health sector has initiated a promising revolution in the area of health care. However, like in all other IT sectors, security issues are of primary concern in e-health care systems. In the present study, considering the Indian e-health scenario we have proposed a model, which integrates the authorization (role based and attribute based) and authentication techniques simultaneously. The suggested model utilizes "Aadhaar" an upcoming identification proof provided by UIDAI (Unique Identification Authority of India) an agency of Government Of India along with spatial &Temporal constraints for the purpose of authentication. Further we have also designed an algorithm for the implementation of same.

Keywords- Authorization and authentication, Aadhaar, UIDAI

I. INTRODUCTION

The advances in medical sciences and ICT (Information and Communication Technologies) are offering wide opportunities for improved health care. Electronic health is a new and efficient method for providing health care services to the society. ICT is playing a crucial role in improving the performance of health care system in the developing countries.

India is a vast country consisting of 28 states and seven union territories. Health is the primary responsibility of each state and there is paucity of infrastructure and dearth of doctors in rural areas. A survey by the Indian medical society has found 75% of qualified consulting doctors practice in urban centers and 23 % in semi urban areas and only 2% from rural areas whereas majority of the patients come from rural areas [1]. Besides, there is no national health insurance scheme in the country. India has emerged as the leader in telemedicine with 380 plus telemedicine centers operating across the country for providing healthcare services to remote areas but unfortunately the percentage of active services are very less. Out of many challenges like poor reach of ICT services in rural areas, low literacy leading to low awareness, insufficient infrastructure, poverty, poor data management is also one of the major deterrents to large scale adoption of e-health. Efforts are directed towards setting up standards and IT enabled healthcare infrastructure in the country. Government, administrative bodies and the different players in the health service system are looking for innovative solutions to make health services most efficient and secure.

In spite of many problems, it is heartening to note that India is among those developing nations, where the progress in e-health has been encouraging. On this front, India is much better placed than other developing nations. The gap is not so much in terms of technical knowledge and actual infrastructure. Organizations like AIIMS, Apollo Hospital, CSIR, CDAC, SGPGI, ISRO, DIT are some of the major players in taking the initiatives. Some of the recent e-health implemented projects include:

• Cloud Enabled E-health Center: India's first fully integrated cloud based e-health center was launched on 1st December 2012 at the Chausala village in Haryana Kaithal District. It was a joint effort of Council Of Scientific Research and Industrial Research (CSIR) and Hewlett Packard. It was set up to provide affordable health services to remote areas.

• Virtual Medical Kiosk:- E-health Access Pvt. Ltd, a healthcare based company launched Virtual Medical Kiosk, which enables patient-doctor consultation in a secure environment. Patients and doctors can communicate through phone, web cams, video conferencing, messaging, or chat.

• Alcohol Web India:- An ehealth portal on alcohol use was developed by National Drug Dependence Treatment Centre(NDDTC) New Delhi as part of an initiative by the WHO, Geneva. The aim of this ehealth portal is to address the problem of alcohol use.

• RFID Individual Tracking and Records Management (RFID-ITRM) e-health project at Ahemdabad, Gujrat:-IEEE launched this project successfully in Ahmedabad. RFID-ITRM technology is central to preventing medical errors, identifying victims of natural disasters, and tracking and monitoring diseases and outbreaks, as well as infants and vaccination history. An electronic medical record system is installed in a local community health care center. The system is managed by local NGO Manav Sadhna.

• E-health Project at Punjab:- An e-health clinic was established in Punjab in Malwa region. A Hyderabad based NGO Naandi Foundation played a major role in launching this project. This e-health clinic offers wide range of medical

services for chronic disease like cancer apart from specialized health care services through telemedicine and broadband electronics methodology.

Besides this, the most important initiative being taken is standardization of exchange of health information between different entities within the healthcare sector. In this regard the ministry of health & family welfare and the ministry of communication and information technology are jointly creating a national health information infrastructure for easy capture and dissemination of health information [1]. Recently the government has also introduced National Health Portal (NHP) scheduled to be launched soon [2].

The NHP is a Union Ministry of Health and Family Welfare Project. The portal is intended to plug in the healthcare gaps through the effective use of IT. It will establish a national database for the medical records of all the citizens from birth to death. The three main objectives of NHP are:-

1. To improve the health awareness among the masses of India.

2. Improvement in the access to health services across the country.

3. Decrease the burden of disease by educating people on the preventive aspects of disease.

The NHP's main aim should be to reach and serve the 330 million Indians below poverty line through innovative ways. The challenge is that nearly 300 million of them are illiterate and less than one percent of them are reachable via internet.

The rest of the paper is structured as follows: In section II, a brief description about Aadhar card is given. In section III, we discuss the security issues in e-health services. In section IV, we give the proposed algorithm and finally the paper concludes with section V.

II. ABOUT AADHAAR

Aadhaar is a 12 digit unique identification number provided by UIDAI (Unique Identification Authority of India-A Government Body under Planning Commission Of India, established in 1999). It is based on the demographic and biometric information. This will ensure that the data collected is clean from the beginning of the program. The UIDIA will be the regulatory authority managing a central identification repository (CIDR) which will issue Aadhaar, update resident information and authenticate the identity of the resident's whenever required[3]. There is a process to ensure that there will be no duplicate records. Residents have only one chance to be in the database. So the individuals are required to provide accurate data as many benefits and entitlement are going to be linked in future and "Aadhaar" will over time be recognized and accepted across the country and across all service providers. Efforts have already been started in introducing "Aadhaar" cards at school and college level. The University Grants Commission (UGC) has issued a letter to the State universities to enroll students for the Unique Identity Card [4]. Linking Aadhaar with students' bank accounts would help in disbursal of scholarships and fellowships. The education department is also taking initiative in enrolling the teaching and non-teaching staff for the Aadhaar card.

A. Security and Privacy in "Aadhaar"

1. Online Authentication:- The UIDAI will provide a strong form of online authentication where the private and public agencies can compare demographic and biometric information of the resident with the record stored in the central database. It will answer all the request to authenticate identity only through a 'Yes' or 'No' response. For example banks can link the unique number to a bank account for every resident, and use the online authentication to allow its customer to access the account from anywhere in the country.
2. Data Transparency:- All the aggregated data shall be available for public to access under RTI (Right to information act) but the Personal Identity Information(PII) will not be accessible by any entity [3].

B. "Aadhaar" in Ehealth Services

The inclusion of Aadhaar will provide a strong authentication in e-health services. Several proposals have been given in integrating UID with Indian health services [5]. Besides this the Ministry of family and healthcare has also planned to integrate "Aadhaar" with NHP in the near future.

III. SECURITY ISSUES IN E-HEALTH IMPLEMENTATION

The use of ICT in the delivery of medical services has given a new horizon to the health sector. The deployment of secured and reliable health information in e-health scenario is a major concern. With the growing use of web based security privacy issues are rising over traditional medical services [6,7]. E-health services are subjected to same security threats as other online services. The National Research Council in 1997 identified five classes of threats to consider for health care systems. They are insiders who make innocent mistakes and cause accidental disclosure of confidential information, insiders who knowingly access information through spite or profit, an unauthorized physical intruder who gains access to information and vengeful employees and outsiders.

Health care services have different users like patients, doctors, nurses; official staff etc. and each of them have different roles to play. Access to sensitive medical records should only be provided to the authorized entity. In [8] the authors have described the access control mechanism for protecting the privacy of patients' records. The access control mechanism is based on the RBAC (role back access control) model, which focuses on the subjects' job functions. Permission is assigned to the jobs, not directly to the users. But this approach is not practical in health domain. RBAC mechanism is not flexible enough for capturing the dynamic behavior of healthcare applications. For example in emergency situation, if the concerned doctor is out of town, another doctor is needed to attend the patient immediately.

Since the user role is not known in advance, permissions cannot be assigned immediately to another doctor.

The dynamic nature of e-health demands a mechanism for providing different levels of protection according to different scenarios (normal or emergency). The aim of the paper is to discuss the security aspects of e-health systems in terms of authorization and authentication. In the next section we discuss the related work in the authorization and authentication in ehealth services. Further a model and algorithm has been designed for providing authorization and authentication in the flexible environment of e-health.

A. Related Work in Authorization and Authentication

There have been only some approaches in e-health service authentication and authorization. In [9] an authentication protocol is developed based on the timestamps. This protocol heavily relies on clock synchronization of both parties, thus issue of trusting each other's clock becomes a problem. In [10], a workflow access control framework is proposed to provide more flexibility in handling e-health dynamic behavior. The idea is to model each work task in the system as state machines. At each state, the data access permission is granted based on resources required to move on to the next state. For any entities involved, the information of all states statuses are stored in a lookup table to improve processing speed. However this approach consumes a large amount of memory space since an entity must store a copy of the status of all states in the system. In [11], an open trusted health informatics structure (OTHIS) is proposed. OTHIS is a broad architecture that can adapt to different types of security services and mechanisms. However the paper only prescribes a generic protocol design, and how to implement the architecture components are not clear. Authors in [12] have investigated the robustness of an e-health care system with smart card based authentication. Blobel et al. [13] focused on the application security challenges and proposed an architectural approach of security. Their approach allow for the central management of the users, privileges, rules, policies and separation of security management and secure application functions.

Most of the studies are based on strict Role based access control (RBAC). In RBAC the users' role should be known in advance. It is not flexible enough for coping with the dynamic behavior of e-health. The above related work did not give a complete solution to the access control problem, either the implementation part is not clear or the study has focused either on authentication or authorization services. So there is need of integrated framework for authorization and authentication for handling the different situations in e-health service system. Few proposals have also been analyzed where the mutual and sequential impact of authorization and authentication in e-health perspective is discussed. For example, in [14] the author proposes a context-aware approach to access control based on conventional discretionary access control (DAC) and role based access control (RBAC) models. The eTRON (Entity and Economy TRON) architecture makes use of tamper-resistant chips equipped with functions for mutual authentication and encrypted communication which is used for authentication and implementing the DAC-based delegation of access-control rights. In another proposal [15] the authors have proposed an architecture for authorization and authentication for e-health services. This system integrated the role based method and the attribute certificate (or privilege) based method to better suit to the e-health service system. Although design and implementation has been not provided.

E-health exhibits different situations. Keeping this in view, in [16] the authors has suggested two risk adaptive techniques to handle e-health service authentication. 1) Ehealth multifactor authentication joint with RBAC and 2) mutual authentication methodologies are used to handle ehealth services authentication under normal, abnormal and critical situations. The proposed model integrates the authentication and authorization principles along with location & time constraints, since a single approach is not suitable for the dynamic environment of e-health.

IV. THE PROPOSED MODEL

Indian e-health system includes use of passwords, smart cards, biometrics, and PKI private keys for the authentication purpose. E-health has dynamic behavior so single approach is not enough for accessing the health system. Presently there is no such solution that focuses on the mutual and sequential approach for the access control. The proposed model simultaneously utilizes the authorization and authentication principle along with the consideration of different situations (normal or emergency). The user shall be authorized by his role (role based authentication) and then by the assigned privileges. The level of authentication shall be different for different situations. For Normal situation the user will be authenticated only once through UID and one more additional layer of authentication shall be done in case of abnormal situation, which shall be done through spatial and temporal constraints. Consider the case of consulting private medical problem, if the checkup neither take place at the hospital nor at the appointment time , we can suspect something is not right. The concept of spatial and temporal constraints has also been earlier explored in [18]

In the proposed model we have integrated UID for authentication purpose. Although the minimum age for applying "Aadhaar" is five years, the demographic details of the persons changes with time and becomes stable after the age of 15. Therefore at present we shall assume that the age of the user in this model is above 15 years. This concept was earlier explored in the paper [17], which linked "Aadhaar" as a tool for authentication in E-Health. The proposed model is an extension of the previous model, which includes location and time constraints also.

A. Policies for Authorization

Authorization consists of role-based authorization and attribute-based authorization. At first the entities have to be identified (example: patient, GP, specialist, nurse, system administrator etc.) for the invocation of role based authorization, secondly determination and then granting of read/write privileges for each of the different roles (attribute based authorization) . For example: if a patient is suffering

from HIV, his personal should be accessible only to the specialist, not to other entities (General Physician, nurse, system administrator etc.)

Authentication is the process of verifying the identity of a role in an e-health service system. Healthcare services are dynamic in nature. The identities of legitimate users need to be verified cautiously before the access privileges are granted. In this model we have proposed two authentication techniques to handle the flexible nature of health services under normal and abnormal situations in Indian Ehealth services.

• Normal Situation: A patient visits his/her family doctor for regular medical checkup.

B. Authentication process

• Abnormal: A patient wants to consult some private medical problem with the doctor or a patient first sees a refereed specialist. Both the situations do not happen regularly.

In Normal situation after the authorization (role based) ,the authentication of UID(Unique Identification) is done at CIDR and in abnormal situations along with the UID authentication spatial and temporal constraints are also verified .

```
1.[Registration of user]
        Get username, password, role and UID
  If(Username and password are valid)then
2.[Role Based Authorization]
    If(Role==doctor)then
 3. Temporary authorization = true.
 4.[authentication of UID at CIDR]
       If(UID is valid)then
 5.          Formal authorization = true.
 6. [Normal Situation: checking of privileges]
 7.[Grant of Read write permission according to
privileges]
    If(situation is normal)then
      If(verification==read)then
        Allow read
       endif
       If(verification==write)then
         Allow write
       endif
       If(verification==read &&
          verification==write)then
         Allow read and write
        endif
 8. [Not permitted]
       If(verification!=read and
         verification !=write)then
         Can't access the ehealth system
       endif
    Else
```

```
6a.[For abnormal situation: Checking of spatial
&temporal constraints]
    get IP address, Network Adaptor IP, MAC
        address, Time, Date
    set spatial =false
    set temporal = false
    if(IP is in a trust network )then
      if(MAC address is a trust workstation)then
          spatial = true
       endif
     endif
    if(Date is in Work schedule ) then
       if(Time is in Work schedule time ) then
          temporal = true
        endif
      endif
  7a.[Assignment of privileges]
     if(spatial and temporal is true) then
        GoTo 7 & 8
      Else
          Can't access the ehealth system
      endif

     endif
    endif
  endif
```

Figure 1 Algorithm for the proposed model.

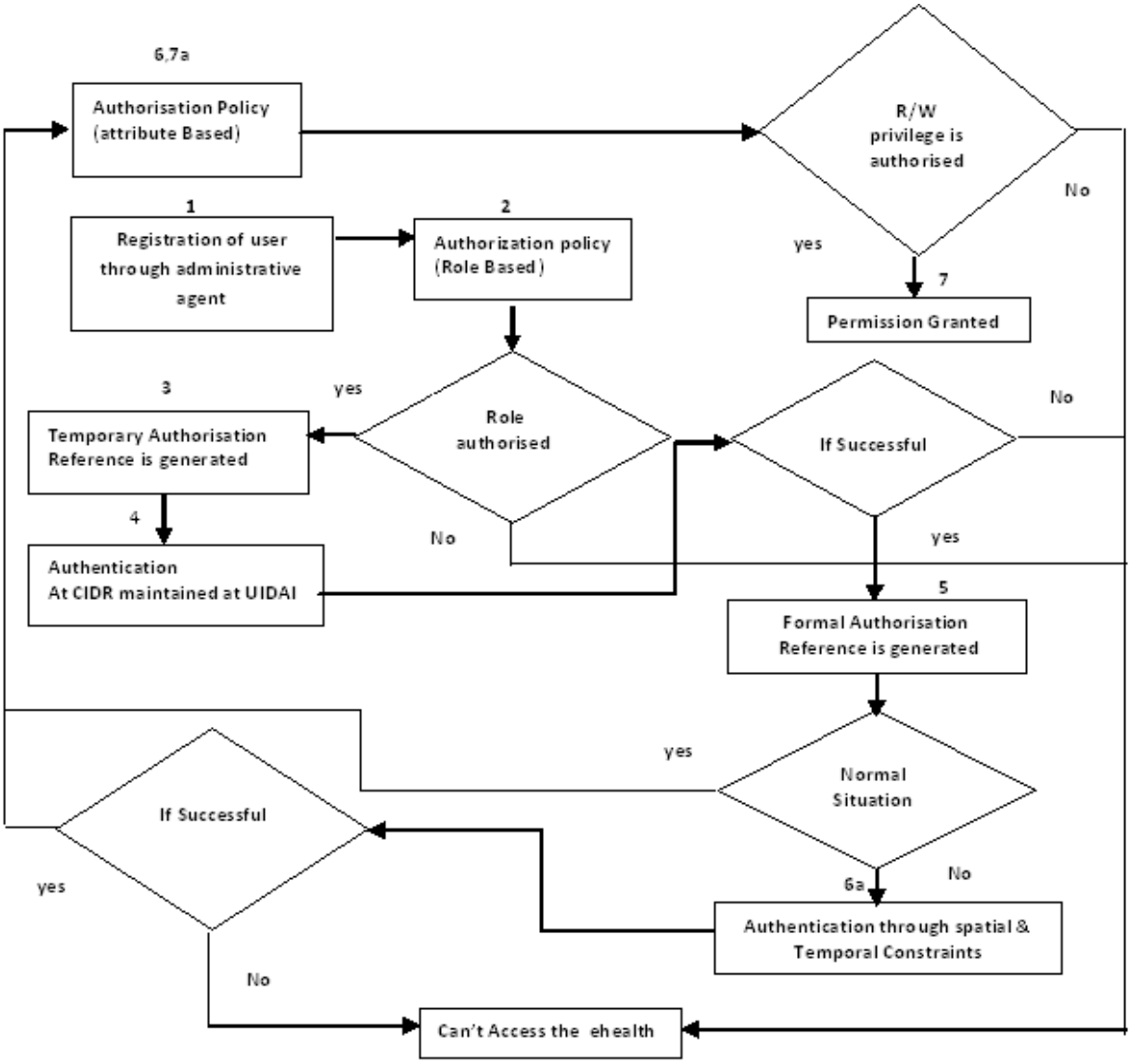

Figure 2 Algorithm for the proposed model.

The algorithm and the flowchart for the events is defined in Figures 1 and 2. This algorithm collects the UID, spatial information; user's proxy IP address and MAC address and temporal information;date and time.We first check the username, password and the role. Only when username, password and the role are verified, we check the UID, spatial and temporal constraints.

V Conclusions and Future Scope

The paper presented the model and algorithm for authentication and authorization of Indian e-health system in normal and abnormal conditions. In normal situation the user is authenticated through "Aadhaar" an upcoming identification proof issued by the UIDAI, Government of India and for abnormal situation an additional layer of security is achieved through time and location parameters. The proposed architecture integrated the role based and privilege based access control. This will ensure to assign different privileges to different roles in the normal and abnormal situations. The flowchart discussed above has been designed from the perspective of a General Physician, the same can be extended for other users (specialist, patient, nurse, staff etc.) considering all the different situations (Normal and abnormal). We shall further implement the prototype of the proposed design for obtaining secured e-health services in terms of authentication and authorization in different situations.

REFERENCES

[1] S K Mishra, Deepak Gupta, Jagdish Kaur ,"Telemedicine in India: Initiatives and vision",9th International Conference on Ehealth Networking Applications and services, Taipei, pp.81-83,19-22 June 2007.

[2] EhealthMagazine,source: http://ehealth.eletsonline.com/2013/06/govt-to-launch-national-health-portal.

[3] http://uidai.gov.in/what-is-aadhaar.html.

[4] http://neg p.gov.in/index.php?option=com_newslatest&view=content.

[5] GpCapt(Dr)Sanjeev Sood(2012), "Aadhaar opening up of new vistas in Healthcare", Ehealth Magazine,January 2012,pp50.

[6] Smith E. Eloff JHP(1999) Security in health care information systems-current trends, International Journal of Medical Informatics, 54:39-54.

[7] Agarwal R, Kini a, LevFevre K, Wang A, Xu Y and Zhou D(2004) Managing Healthcare Data HippocraticallyProc. Of ACM SIGMOD Intl. Conference On Management of Data.

[8] L. Rostad and O.Edsberg(2006), " A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access logs." In Proc. Of 22nd Annual Computer Security Applications Conference, Miami,Florida.

[9] K.Elmufti,D.Weerasinghe,M.Rajarajan,V.Rakocevic,S.Khan, "Timestamp Authentication Protocol for remote Monitoring in ehealth," The 2nd International conference on pervasive computing technologies for healthcare,Tampere,finland,pp.73- 76.

[10] G. Russello C.Dong,N.Dulay(2008),"A Workflow based access control framework for ehealth application",proc. of the 22nd International conference on advanced information networking and applications-workshops,pp.111-120.

[11] V.Liu,W.Caelli,L.May,P.Croll(2008),"OpenTrusted Health Informatics Structure, (OTHIS),"Proc. of the 2nd Australian Workshop on Health Data Knowledge Management, Vol.80,pp.33-43.

[12] Kuo-Hui Yeh, N.W. Lo, Tzong-Chen Wu, Ta-Chi Yang and Horng-Twu Liaw(2012), " Analysis of an e-Health care system with Smart Card Based Authentication", Seventh Asia Joint Conference on Information Security, Hualien, Taiwan,pp 59-61.

[13] Blobel et al.(2006)," Alerts in Clinical Information Systems: Building Frameworks and Prototypes ", Proc. Of AMIA Fall Symposium, Washington D.C.

[14] Khan, M. Fahim Ferdous(2012)," Context aware access control for clinical information system",International Conference on Innovations in Information Technology(IIT), Tokyo, Japan, pp.123-128.

[15] Song Han, Geoff.Skinner,Vidyasagar.Potdar, Elizabeth.Chang(2004) ,"A Framework of Authentication and Authorization for e-Health Services",Proceedings of the UK e- Science All Hands Conference 2004.

[16] Apaporn Boonyarattephan, Yan Bai,Sam chung(2009),"Security Framework for e-Health Service Authentication and e-Health Data Transmission(2009)",9th International Symposium On Communications and Information Technology.ISCIT 2009.pp1213-1218,28-30 .

[17] Apaporn Boonyarattaphan, Yan Bai, Sam Chung and Radha Poovendran, " Spatial - Temporal Access Control for e-Health Services." Fifth International Conference on Networking , Architecture and storage.pp.269 - 276,15-17 July 2010.

[18] Shilpa Srivastava, Namrata Agarwal, Ritu Agarwal," Authenticating Indian E-health System through "Aadhaar" A unique Identification", IJSER, ISSN 2229-5518,Volume 4 Issue 6, pp 2412-2416.