Authenticating Indian E-Health System Through "Aadhaar" A Unique Identification

Shilpa Srivastava*
Ritu Agarwal*

Abstract

Implementation of an e-health care system without compromising the security is of primary concern. The technological barriers in the successful deployment of e-health services in India have been analyzed . The article focuses on the need of simultaneous approach of authorization and authentication. Further a model has been proposed for providing secured e-health services in India. The model makes use of "Aadhaar" for authentication purpose. "Aadhaar" is a twelve digit unique identification number provided by UIDAI (Unique Identification Authority of India), an agency of Government of India.

Keywords: Authorization and authentication, Aadhaar, UIDAI

Introduction

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 [Smith E. Eloff JHP (1999); Agarwal R, Kini a, LevFevre K, Wang A, Xu Y and Zhou D (2004)]. 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. Rostad L. and Edsberg O. (2006) 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. Permissions are assigned to the jobs, not directly to the users. But this

*MCA Department, RKGIT, Uttar Pradesh Technical University, Lucknow, Uttar Pradesh, India.

Authors are grateful to the anonymous referees for comments and suggestions for improving the text and contents of the paper. Authors alone are responsible for any errors/mistakes still remaining in the paper.

approach is not practical in health domain. RBAC mechanism is not flexible enough for capturing the dynamic behavior of healthcare applications. For example, in an 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 can not 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, some recent e-health initiatives in Indian Context have been discussed. Security issues have also been analyzed. Further, a model has been designed for providing authorization and authentication in the flexible environment of e-health. This model is based on "Aadhaar", a unique identification provided by UIDAI .

E-Health in Indian Context

India is acquiring a sizable market in health care. Apollo Hospital, CSIR, CDAC, SGPGI, ISRO, DIT are some of the major players in the implementation of e-health. Some of the recent e-health initiatives are:

- **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 Kaithal District of Haryana. It was a joint effort of Council Of Scientific Research and Industrial Research(CSIR) and Hewlett Packard. The purpose of this project is to facilitate preliminary and affordable healthcare in remote rural regions.
- **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. Fig.1 is the image of the device which can be installed in a variety of places: in a corporate for employee use, at a retail store, old age homes, or even in a gated community [URL: http://bussinesswireindia.com/PressRelease.asp].

Figure 1: Virtual Medical Kiosk

Figure 2: E-health care workers at the clinic

- **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. Fig. 2 is the image of the clinic[URL: http://sites.ieee.org/societies/2012/05/ 09/ieee - launches-major-e-health-pilot-in-india, 2012].
- **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 broad band electronics methodology.

Technical challenges in wide deployment of E-health

India is a developing country consisting of 29 states and six union territories. Health is the primary responsibility of each state and there is paucity of infrastructure and dearth of doctors in rural areas. Besides, there is no national health insurance policy for the country. India has emerged as the leader in telemedicine with 400 plus telemedicine centers operating across the country for providing healthcare services to remote areas but unfortunately less than 50% of these services are active now. Out of many challenges like education, poverty, financial resources, secured data management is also of primary concern. Poor data management is one of the major problems in the developing countries which leads to breaches in data security and therefore it is considered as one of the major deterrents to the 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. One of 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 [Mishra, S.K]. The center shall soon establish a national database for the medical records of all the citizens from birth to death that will come out with the launch of a National Health Portal [URL: http://ehealth.eletsonline.com/2011/06/national-Health-portal-for-india]. Efforts are also being made to use "Aadhaar" in the health care system [Sanjeev Sood (2012); Shweta Kannan (2013)].

The Proposed Model

Authentication options in Indian e-health system includes use of passwords, smart cards, biometrics, and PKI private keys [Ganapathy K. (2008)]. E-health has dynamic behavior so is a need of mutual and sequential approach of access control. 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). It will integrate the role based method and attribute certification and the basis of authentication shall be the "Aadhaar".

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 Aadhar, update resident information and authenticate the identity of the resident whenever required. The inclusion of Aadhaar will provide a strong authentication in e-health services. Soon the Aadhaar cards will be mandatory for university and college students. The UIDAI plans to enroll residents into its database with proper verification of their demographic and biometric information. Aadhaar will over time be recognized and accepted across the country and across all service providers.

Related Work in Authorization and Authentication

There have been some approaches in e-health service authentication and authorization.

Elmufti K., Weerasinghe D., Rajarajan M., Rakocevic V. and Khan S. (2008) have developed an authentication protocol 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.

G. Russello C. Dong, N. Dulay (2008) proposed a workflow access control framework 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.

Liu V., Caelli W., May L. and Croll P. (2008), an open trusted health informatics structure (OTHIS) proposal. 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.

Kuo-Hui Yeh, N.W. Lo, Tzong-Chen Wu, Ta-Chi Yang and Horng-Twu Liaw (2012) have investigated the robustness of an e-health care system with smart card based authentication.

Blobel et al. [Blobel et al. (2006)] focused on the application of 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; Khan, M. Fahim Ferdous (2012) 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, Song Han, Geoff. Skinner, Vidyasagar. Potdar, Elizabeth. Chang (2004) 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, [Apaporn Boonyarattephan, Yan Bai, Sam Chung (2009)] the authors has suggested two risk adaptive techniques to handle e-health service authentication under normal, abnormal and critical situations.

The proposed model integrates the authentication and authorization principles as a single approach is not suitable for the dynamic environment of e-health.

Policies for Authorization

Authorization consists of role based authorization and attribute based authorization. At first, the stakeholders 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), is one for example: if a patient is suffering from HIV, his personal data should be accessible only to the specialist, not to other entities (General Physician, nurse, system administrator etc.)

Authentication process

Authentication is the process of verifying the identity of a role in an e-health service system. In the proposed system, each role of the underlying service system will be authenticated on the basis of "Aadhar". Although the minimum age for applying "Aadhaar" is five years but since the demographic details of the person changes with time and becomes stable after the age of 15, we shall assume that the age of the user in this model is above 15 years.

Simultaneous approach for authentication and authorization:-

In the e-health system, the users can be General Physician, Nurse, Specialists and a number of patients. E-health is a dynamic domain in which different privileges are associated with different roles. The dynamicity further increases with the different situations (normal and emergency). The flow of events in the proposed model has been designed from the perspective of a general physician in normal and emergency scenario. The steps for the authentication and authorization are as follows:-

1. The user first registers himself/herself with the e-health service system through administrative agent.
2. The administrative first checks the role of the user. If it an authorized role ie; GP, Patient, Nurse or Specialist then only primitive authorization reference will be generated otherwise the user can't access the e-health service system (role based authorization).
3. After getting the temporary authorization reference number, the user is asked to provide the "Aadhaar" number.
4. The identity of the user is authenticated online at CIDR (Center Identification repository) maintained at UIDAI.
5. If the authentication is successful, formal authorization reference will be generated.
6. If the situation is normal, the user is verified for the different privileges (reading/writing) into the e-health service System (attribute certification).
7. If the status of the user is satisfied according to the authorization policy, then he will be granted permission to access the relevant record.
8. If the situation is not normal like in emergency, multiple levels of authentication and authorization are required. The general physician is required to authenticate himself/herself through emergency identification number provided from the office of Chief Medical Officer.
9. If this authentication is successful, the user is verified for different privileges (reading/writing) into the e-health System (attribute certification).
10. If the privilege is authorized, permission is granted for accessing the e-health system.

Fig 3 illustrates the complete flow of events of the proposed model.

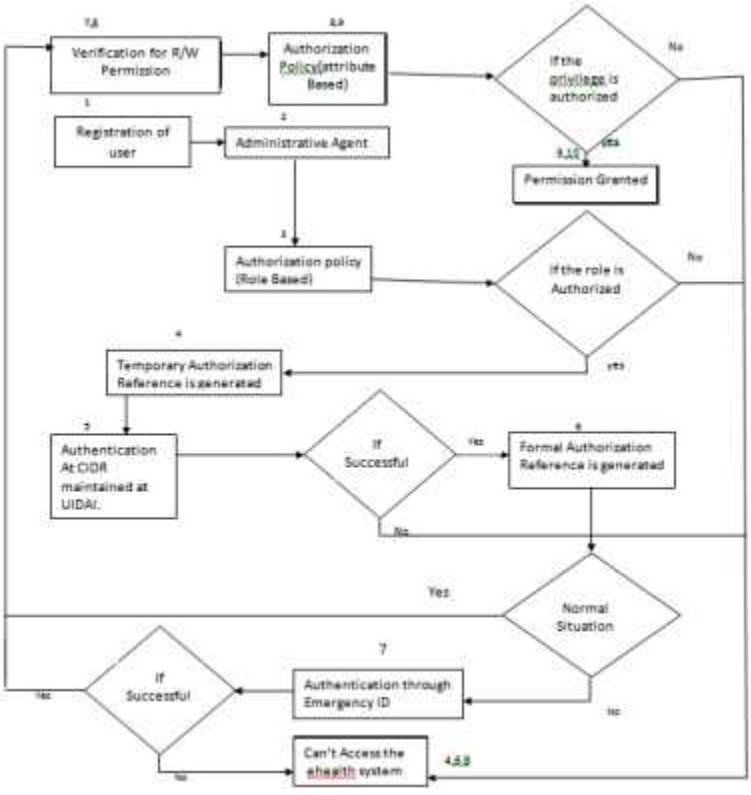

Figure 3: The proposed model

Conclusion and Future Scope

The paper presented the model for authentication and authorization of Indian e-health system through "Aadhaar"- an upcoming identification proof issued by the UIDAI, Government of India. 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 critical 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.) also. In the next step we shall implement the prototype of the proposed design for obtaining a secured e-health services in terms of authentication and authorization in different situations.

References

1. *Smith E. Eloff JHP (1999), Security in health care information systems-current trends, International Journal of Medical Informatics, 54:39-54.*
2. *Agarwal R, Kini a, Lev Fevre K, Wang A, Xu Y and Zhou D (2004) Managing Healthcare Data Hippocratically Proc. Of ACM SIGMOD Intl. Conference On Management of Data.*
3. *Rostad L. and Edsberg O. (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.*
4. *http://bussinesswireindia.com/PressRelease.asp, November2012*
5. *http://sites.ieee.org/societies/2012/05/09/ieee-launches-major-e-health-pilot-in-india, 2012.*
6. *Dr. S.K. Mishra, "Ehealth initiatives in India", http://openmed.nic.in/1265/01/skm12.pdf*
7. *http://ehealth.eletsonline.com/2011/06/national-Health-portal-for-india.*
8. GpCapt (Dr) Sanjeev Sood (2012), *http://ehealth.eletsonline.com/2012/01/aadhaar-opening-up-of-new-vistas-in-healthcare-gp-capt-dr-sanjeev-sood-hospital-administrator-and-nabh-empanelled-assessor/.*
9. *Shweta Kannan (February 2013), Retrieved from "http://www.thehindubusinessonline.com/companies/apollo-hospitals-working-on-linking-ehealth-records-with-Aadhaar.*
10. *Ganapathy K. (2008), Retrieved from http://conf.isi.qut.edu.au, 2008.*
11. *Elmufti K., Weerasinghe D., Rajarajan M., Rakocevic V. and Khan S. (2008), "Timestamp Authentication Protocol for remote Monitoring in ehealth," The 2nd International conference on pervasive computing technologies for healthcare, Tampere, finland, pp. 73- 76.*
12. *Russello G., Dong C. and Dulay N. (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.*
13. *Liu V., Caelli W., May L. and Croll P. (2008), "Open Trusted Health Informatics Structure, (OTHIS)," Proc. of the 2nd Australian Workshop on Health Data Knowledge Management, Vol. 80, pp. 33-43.*
14. *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.*
15. *Blobel et al.(2006)," Alerts in Clinical Information Systems: Building Frameworks and Prototypes", Proc. Of AMIA Fall Symposium, Washington D.C.*
16. *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.*
17. *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 website: http://www.allhands.org.uk/2004/*
18. *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. pp 1213-1218, 28-30.*