Anonymous Authentication Scheme for Smart

Cloud Based Healthcare Applications

INTRODUCTION

Recent advances in biosensors, wireless network and embedded systems have assisted the rapid development of a wide range of wearable and implantable sensors in the human body. To collect crucial health data such as blood pressure level, and heart rate, many smart phone based health applications have been developed in the recent past [1], [2]. The data from the sensors is sent to the cloud server, where hospitals have hosted their services for data processing. The data is analyzed to improve the level of healthcare given to the patients. An example of smart cloud based health applications is shown in Fig. 1. Ideally, patients want hospitals to assist them with high efficiency without revealing patients’ identities.The increasing necessity for massive computation and excessive amounts of storage, is driving the healthcare industry to use cloud based servers, because of many advantages they are offering, such as cost saving and scalability.

**OBJECTIVE**

The performance of our scheme is evaluated by theoretical analysis which demonstrates that it resists various attacks and provides several attractive security features.

**EXISTING CONCEPT:-**

In existing system now a days in hospitals lot of patients are coming to hospital the hospital management don’t know weather who is coming to admit in hospital how is going to register they are not identifying. And what is the problem also they do not understand clearly. If any emergency case is there they are not getting operation at correct time to overcome all those problems we are going to implement some methods in proposed system.

**Disadvantages:**

Patient may lose life.

**LITERATURE SURVEY**

**TITLE:** The pursuit of citizens’ privacy: a privacy aware smart city is possible

**AUTHOR:** Martinez-Balleste, P. A. Perez-Martinez, and A. Solanas,

**YEAR: 2013**

**DESCRIPTION:**

Cities are growing steadily, and the process of urbanization is a common trend in the world. Although cities are getting bigger, they are not necessarily getting better. With the aim to provide citizens with a better place to live, a new concept of a city was born: the smart city. The real meaning of smart city is not strictly defined, but it has gained much attention, and many cities are taking action in order to be considered 'smart'. These smart cities, founded on the use of information and communication technologies, aim at tackling many local problems, from local economy and transportation to quality of life and e-governance. Although technology helps to solve many of these local problems, their ability to gather unprecedented amounts of information could endanger the privacy of citizens. In this article we identify a number of privacy breaches that can appear within the context of smart cities and their services. We leverage some concepts of previously defined privacy models and define the concept of citizens' privacy as a model with five dimensions: identity privacy, query privacy, location privacy, footprint privacy and owner privacy. By means of several examples of smart city services, we define each privacy dimension and show how existing privacy enhancing technologies could be used to preserve citizens' privacy.

**TITLE:** Real time tele-monitoring of patients with chronic heart-failure using a smartphone: lessons learned

**AUTHOR:** D. Aranki, G. Kurillo, P. Yan, D. M. Liebovitz, and R. Bajcsy

**YEAR:** 2016

**DESCRIPTION:**

We present a smartphone-based system for real-time tele-monitoring of physical activity in patients with chronic heart-failure (CHF). We recently completed a pilot study with 15 subjects to evaluate the feasibility of the proposed monitoring in the real world and examine its requirements, privacy implications, usability, and other challenges encountered by the participants and healthcare providers. Our tele-monitoring system was designed to assess patient activity via minute-by-minute energy expenditure (EE) estimated from accelerometry. In addition, we tracked relative user location via global positioning system (GPS) to track outdoors activity and measure walking distance. The system also administered daily surveys to inquire about vital signs and general cardiovascular symptoms. The collected data were securely transmitted to a central server where they were analyzed in real time and were accessible to the study medical staff to monitor patient health status and provide medical intervention if needed. Although the system was designed for tele-monitoring individuals with CHF, the challenges, privacy considerations, and lessons learned from this pilot study apply to other chronic health conditions, such as diabetes and hypertension, that would benefit from continuous monitoring through mobile-health (mHealth) technologies.

**TITLE:** Security and privacy in cloud computing

**AUTHOR:** Z. Xiao and Y. Xiao,

**YEAR:2013**

**DESCRIPTION:** Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in all the globe. Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture. This study is to review different security techniques and challenges from both software and hardware aspects for protecting data in the cloud and aims at enhancing the data security and privacy protection for the trustworthy cloud environment. In this paper, we make a comparative research analysis of the existing research work regarding the data security and privacy protection techniques used in the cloud computing.

**TITLE:** A smart health application and its related privacy issues

**AUTHOR:** D. Ding, M. Conti, and A. Solanas,

**YEAR: 2016**

**DESCRIPTION:**

Together with the development of technologies such as those for ubiquitous computing, data mining, Internet of Things (IoT) and wireless sensor networks (WSNs), the concepts of smart cities and mobile health (m-Health) have emerged. Along the same line, the smart health concept (s-Health), understood as a context-aware healthcare paradigm for smart environments, improves the quality of healthcare systems within smart cities. However, s-Health may encounter some privacy and security issues. For example, in order to obtain the current location and health conditions of citizens, these citizens might be continuously monitored, which could be seen as a privacy invasion. In this paper, we describe an application within the s-Health paradigm. In particular, our approach allows to effectively deal with citizens who have respiratory conditions. Our application example suggests low-pollution routes to citizens in order to lessen their respiratory-related problems, and proactively activates water sprays in fountains to reduce the effect of pollution or pollen. Besides the description of the application, the main contribution of the article is the analysis of the emerging privacy issues of the proposed application and the discussion of possible countermeasures.

**TITLE:** Untraceable sensor movement in distributed iot infrastructure

**AUTHOR:** P. Gope and T. Hwang

**YEAR: 2015**

**DESCRIPTION:**

Recent advances in information and communication technologies and embedded systems have given rise to a new disruptive technology, the Internet of Things (IoTs). IoT allows people and objects in the physical world as well as data and virtual environments to interact with each other so as to create smart environments, such as smart transport systems, smart cities, smart health, and so on. However, IoT raises some important questions and also introduces new challenges for the security of systems and processes and the privacy of individuals, such as their location and movements and so on. In this paper, at first, we propose a distributed IoT system architecture. Subsequently, we propose an anonymous authentication scheme, which can ensure some of the notable properties, such as sensor anonymity, sensor untraceability, resistance to replay attacks, cloning attacks, and so on. It is argued that the proposed authentication scheme will be useful in many distributed IoT applications (such as radio-frequency identification-based IoT system, Biosensor-based IoT healthcare system, and so on), where the privacy of the sensor movement is greatly desirable.

**TITLE:** Privacy as a service: Protecting the individual in healthcare data processing

**AUTHOR:** X. Su, J. Hyysalo, M. Rautiainen, J. Riekki, J. Sauvola, A. I. Maarala, H. Hirvonsalo, P. Li, and H. Honko,

**YEAR:** 2016

**DESCRIPTION:**

Health applications involve many data sources, individuals, and services that work against guarantees that an individual's personal data will not be used without consent. The proposed privacy-centered architecture integrates data security and semantic descriptions into a trust-query framework, enabling the provision of user consent as a service.

**TITLE:** A secure anonymous authentication scheme for electronic medical records system

**AUTHOR:** W. Lei, Y. Li, Y. Sang, and H. Shen,

**YEAR:** 2016

**DESCRIPTION:**

Based on smart devices and wireless communication infrastructure, the Electronic Medical Records (EMR) systems become more and more popular in hospitals by reason of its convenient operation, remote access, data integrity, facilitated resources sharing, statistical analysis and many other advantages. When entering an EMR system, patients can be treated by many kinds of services and also leave their privacy to the providers. It is a viable method to protect a patient's privacy in EMR by anonymous authentication, where identity of the patient is verified without demonstrating the true identity to the authenticator. This paper proposes an enhanced secure anonymous authentication scheme, based on smart card and biometrics with key agreement. According to security analysis, our scheme is secure against many types of attacks, including those not prevented by previous work, such as the smart card loss attack and impersonation attack. The performance of our scheme is also analyzed and compared with previous work, which shows that our scheme is more efficient in the computation cost.

**TITLE:** Consumer oriented privacy preserving access control for electronic health records in the cloud

**AUTHOR:** R. Fernando, R. Ranchal, B. An, L. B. Othman, and B. Bhargava,

**YEAR:** 2016

**DESCRIPTION:**

This paper addresses privacy issues in managing electronic health records by a third party cloud based service. Compared to traditional authentication-authorization mechanisms, the proposed approach minimizes the leakage of identity information of involved participants through unlinkability. Furthermore, it gives the ability to health record owners for making access control decisions. This solution employs an identity management scheme that enhances consumer privacy by preventing consumer profiling based on the credentials used to satisfy the service provider policies. The paper proposes a set of mechanisms to allow authenticated unlinkable access to electronic health records, while giving the record owners ability to make access control decisions. The security evaluation for accessing data in the cloud is detailed, and the implementation of the system is evaluated in this paper.

**PROPOSED CONCEPT:-**

* In proposed system to overcome all these type of problems while joining to hospital they have to register first .
* After registration admin will provide one id to that patient. by using that id they have to login.
* After login of that page where is one menu under that for that patient what the user need they have to send a request to admin for what the requirement they need .
* If admin will receive that request. Immediately .they will respond and they will provide concernperson .

In this project we have the following modules:

1. **User Interface**
2. **Group Manager**
3. **User**
4. **Cloud Service Provider**
5. **Services**

**User Interface:**

This is the first module of our project. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password we can’t enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

Database

Welcome Page

Registration

Page

Login

Server

Username Yes

Verify

Password

No

**Group Manager**

Group Manager is a first module of this project. This GM is the owner of the hospital. In this module GM login, and then view the all users request and accept the users and generate ID to that users. GM sends accepted user’s details to cloud service provider to provide the hospital services to the users. And GM also add the doctors based on the diseases. He can view the total doctors details.

Login

Verify

Error page

Home Page

Accept Request

Sends User ID to CSP

Generate ID to user

Logout

View Doctors

Invalid

Valid

**User:**

User is the second module of this project. In this module user can register with Group Manager. Send request to get the ID after getting ID user can login to the site, send request to the Cloud Service Provider to access the hospital services. After receiving the key from CSP, user can use the services. If the user is authenticated then only he can use the services otherwise that user is deleted/removed by the CSP.

Register / Login

Verify

Error page

Home Page

Send request to CSP for Key

Send request to GM for ID

Use the services provided by the GM

View First Aid Information

**Cloud Service Provider**

Cloud Service Provider is the third module of the project. CSP login and he can view the patient request , if the patient is authorized then only key will generated to the patient otherwise he can removed without using the services.

Login

Verify

Error page

Home Page

Accept Request

Provide services

Generate key to user

Logout

View ID’s

5. Services

Services are the fourth module of the project. In this module patient can login into the services page and he can view the services provided by the GM/Hospital based on his requirement he can send request to the particular service to access.

Provide Patient ID & Secret Code

Logout

Access the Service

Send request to Doctor

**Given Input and Expected output**

User Interface Design

Input : Enter Login name and Password

Output : If valid user name and password then directly open the home page otherwise show error message and redirect to the registration page.

User

Input : login and send request to GM and CSP

Output: get ID and key then use the services provided by the GM / Hospital

Gm

Input : login and view user request and add doctors

Output : Control the services and view doctors.

 CSP

Input : login and view requests of the users

Output : generate key to the user give permission to access services

services

Input : ID and key

Output: view the services and use the services

**MINIMUM SYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUOS.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE

**UML Diagrams**

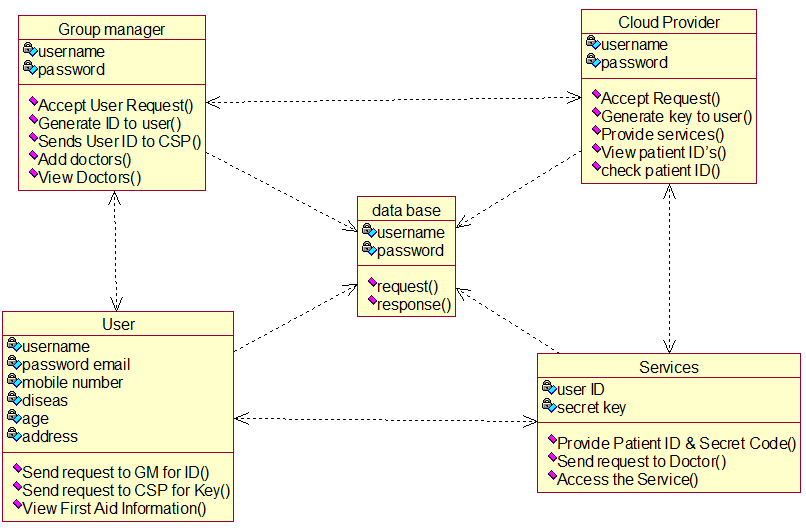
**Use Case Diagram**

****

**EXPLANATION:**

The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted. The above diagram consists of user as actor. Each will play a certain role to achieve the concept.

**Class Diagram**



**EXPLANATION**

In this class diagram represents how the classes with attributes and methods are linked together to perform the verification with security. From the above diagram shown the various classes involved in our project.

**State Diagram**

****

**EXPLANATION:**

State diagram are a loosely defined diagram to show workflows of stepwise activities and actions, with support for choice, iteration and concurrency. State diagrams require that the system described is composed of a finite number of states; sometimes, this is indeed the case, while at other times this is a reasonable abstraction. Many forms of state diagrams exist, which differ slightly and have different semantics.

**Activity Diagram**



**EXPLANATION:**

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

**Sequence Diagram**



**EXPLANATION:**

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

**Collaboration Diagram**



**EXPLANATION:**

A collaboration diagram, also called a communication diagram or interaction diagram, is an illustration of the relationships and interactions among software objects in the Unified Modeling Language (UML). The concept is more than a decade old although it has been refined as modeling paradigms have evolved.

..

**Object Diagram**

****

**EXPLANATION:**

In the above digram tells about the flow of objects between the classes. It is a diagram that shows a complete or partial view of the structure of a modeled system. In this object diagram represents how the classes with attributes and methods are linked together to perform the verification with security

**Deployment Diagram**



**Component Diagram**



Data Flow Diagram

**DB**

Login

Provide ID

View request

View Doctors

Add Doctors

**DB**

Access services

Send request to CSP

Get ID from GM

Send request to GM

Enter ID &Key

View services

Get key from CSP

Login

Provide services to user

View request

Login

Generate key to user

E-R Diagram

Send request to

Group manager

View user request

Generate ID to user

Send request to

CSP

Check user ID’s

Generate Secret key to user

Enter key and ID

Access Services

User

**System Architecture:**

Login

Provide ID

View request

View Doctors

Add Doctors

**DB**

View patient ID’s

View request

Login

Accept Request

Access services

Send request to CSP

Get ID from GM

Send request to GM

Enter ID &Key

View services

Get key from CSP

Login

Provide Patient ID & Secret Code

Book the Doctor

Send request to Doctor

Check patient ID

Provide services

**CONCLUSION**

Protecting the privacy of patients is crucial to the success of smart cloud based healthcare applications. In this paper, we have presented the anonymous authentication scheme for smart cloud based healthcare applications. The proposed scheme preserves the privacy of patients when they access the services hosted on the cloud. The scheme utilizes rotating group signature scheme based on ECC. Due to smaller key sizes used in ECC, the security of the system can be easily scaled up by increasing the key size without affecting the computational complexity. The scheme adds an extra layer of protection against traffic analysis attacks by an eavesdropper by providing anonymity at the network layer by employing TOR. The scheme protects patients’ sensitive data from an eavesdropper and untrusted cloud servers. One salient feature of our scheme is that the medical application or service providers cannot reveal the identity of the patient hence protecting the privacy. In this paper, we have designed a practical system which is

secure and efficient. The proposed authentication scheme ensures that the patients can consume services without revealing their identity at the time of consumption or retrospectively.

**REFERENCE**

[1] A. Martinez-Balleste, P. A. Perez-Martinez, and A. Solanas, “The pursuit of citizens’ privacy: a privacy aware smart city is possible,” IEEE Commun. Magazine, vol. 51, no. 6, pp. 136–141, Jun. 2013.

[2] D. Aranki, G. Kurillo, P. Yan, D. M. Liebovitz, and R. Bajcsy, “Realtime tele-monitoring of patients with chronic heart-failure using a smartphone: lessons learned,” IEEE Trans. on Affective Computing, vol. 7, no. 3, pp. 206–219, Apr. 2016.

[3] Z. Xiao and Y. Xiao, “Security and privacy in cloud computing,” IEEE Commun. Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, May 2013.

[4] D. Ding, M. Conti, and A. Solanas, “A smart health application and its related privacy issues,” in Proc. Smart City Security and Privacy Workshop (SCSP-W), Apr. 2016, pp. 1–5.

[5] P. Gope and T. Hwang, “Untraceable sensor movement in distributed iot infrastructure,” IEEE Sensors J., vol. 15, no. 9, pp. 5340–5348, Jun. 2015.

[6] X. Su, J. Hyysalo, M. Rautiainen, J. Riekki, J. Sauvola, A. I. Maarala, H. Hirvonsalo, P. Li, and H. Honko, “Privacy as a service: Protecting the individual in healthcare data processing,” Comput., vol. 49, no. 11, pp. 49–59, Nov. 2016.

[7] W. Lei, Y. Li, Y. Sang, and H. Shen, “A secure anonymous authentication scheme for electronic medical records system,” in Proc. 13th Int. Conf. on e-Business Engineering, Nov. 2016, pp. 48–55.

[8] V. Sucasas, G. Mantas, A. Radwan, and J. Rodriguez, “An oauth2-based protocol with strong user privacy preservation for smart city mobile ehealth apps,” in Proc. IEEE Int. Conf. on Commun., May 2016, pp. 1–6.

[9] R. Fernando, R. Ranchal, B. An, L. B. Othman, and B. Bhargava, “Consumer oriented privacy preserving access control for electronic health records in the cloud,” in Proc. IEEE 9th Int. Conf. on Cloud Computing, Jun. 2016, pp. 608–615.

[10] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, “Protection of big data privacy,” IEEE Access, vol. 4, pp. 1821–1834, Apr. 2016.

[11] H. Xiong, J. Tao, and C. Yuan, “Enabling telecare medical information systems with strong authentication and anonymity,” IEEE Access, vol. 5, pp. 5648–5661, 2017. [12] X. Li, S. Tang, L. Xu, H. Wang, and J. Chen, “Two-factor data access control with efficient revocation for multi-authority cloud storage system,” IEEE Access, vol. 5, pp. 393–405, 2017.

[13] J. Zhu and J. Ma, “A new authentication scheme with anonymity for wireless environments,” IEEE Trans. on Consumer Electron., vol. 50, no. 1, pp. 231–235, Feb. 2004.

[14] G. Horn and B. Preneel, “Authentication and payment in future mobile systems,” Comput. Security – ESORICS 98, pp. 277–293, 1998.

[15] C. Yang, W. Ma, and X. Wang, “Novel remote user authentication scheme using bilinear pairings,” Lecture Notes in Comput. Science, vol. 4610, p. 306, 2007.