Sistema biométrico para control de acceso con doble validación
Biometric system for access control with double validation

Carlos Ignacio Torres-Londoño[1], Juan David Gallego-Giraldo[2], Andrés Felipe Garay-Flórez[3]
[1,2,3]Programa Ingeniería de sistemas, Facultad de Ingeniería, Universidad Cooperativa de Colombia sede Villavicencio, Grupo de Investigación GIPIS
[1] carlos.torreslo@campusucc.edu.co,[2] juan.gallegog@campusucc.edu.co, [3]andres.garay@campusucc.edu.co

Resumen– *Las entidades de salud, tiene áreas de acceso restringido (morgue, quirófanos, etc.) y en algunos casos controlado, los accesos deben quedar registrados en bitácoras de quien ingresa y a qué hora, de ser posible también la hora de salida. El control de los accesos sirve, para evitar riesgos que pueden ir desde contagios, hasta mala manipulación de instrumentos o equipos médicos y pérdidas de información entre otros. ¿Cómo controlar el acceso del personal hacia las diferentes áreas en la clínica de la UCC? El control de accesos y las restricciones a las diferentes áreas de una clínica, son importantes y deben ser una política de la alta dirección; por esta razón desde la clínica de la UCC plantea con la facultad de ingeniería de la UCC el diseñar e implementar un sistemas de control que permita restringir el acceso a diferentes zonas de la clínica según las tareas y responsabilidades de cada miembro. El prototipo electrónico debe permitir la apertura de puertas mediante el uso de tecnología RFID, además del envió de tokens para confirmarla identidad, se desarrolla una aplicación informática para controlar los diferentes accesos a las áreas restringidas de la clínica generando la bitácora que muestra la hora de ingreso y la hora de salida. El sistema debe permitir según el área, el uso de una serie de medidas para el acceso a la misma, no todas las áreas deben tener el mismo nivel de acceso y no todos los usuarios deben poder acceder a todas las áreas.*

Palabras claves– *Control de acceso biometrico, computación ublicua, tarjetas inteigentes, Internet de las cosas.*

Abstract– *Health entities, have restricted access areas (morgue, operating theaters, etc.) and in some cases controlled, access must be recorded in logs of who enters and at what time, if possible also the time of departure. The control of the accesses serves, to avoid risks that can go from contagious diseases, to bad manipulation of instruments or medical equipment and losses of information among others. How to control the access of the personnel to the different areas in the clinic of the UCC? Access control and restrictions to different areas of a clinic are important and should be a policy of senior management; For this reason, from the UCC clinic, the UCC's engineering faculty proposes to design and implement a system of control that allows restricting access to different areas of the clinic according to the tasks and responsibilities of each member. The electronic prototype must allow the opening of doors using RFID technology, in addition to sending tokens to confirm identity, a computer application is developed to control the different accesses to the restricted areas of the clinic generating the logbook that shows the time of Income and the time of departure. The system should allow according to the area, the use of a series of measures for access to it, not all areas should have the same level of access and not all users should be able to access all areas.*

Keywords– *Biometrics (access control), ubiquitous computing, smart cards, internet of things*

1. Introducción

El control de accesos y las restricciones a las diferentes áreas de una clínica, son especialmente importantes y deben ser una política de la alta dirección de la misma; por esta razón desde la clínica de la Universidad Cooperativa se plantea a la facultad de ingeniería de la Universidad Cooperativa de Colombia el diseñar e implementar un sistemas de control que permita restringir el acceso a diferentes zonas de la clínica según las tareas y responsabilidades de cada miembro de la clínica (Rol).

El sistema que se plantea debe tener una serie de factores que permita según el área, el uso de una serie de medidas para el acceso a la misma, no todas las áreas deben tener el mismo nivel de acceso y no todos los usuarios deben poder acceder a todas las áreas; se debe tener en cuenta que en una clínica el acceso a áreas restringidas puede conllevar una serie de factores de riesgo no solo para quien accede a ella sino también para el personal que se

encuentra dentro de esta área. Así es importante controlar en ciertas áreas la circulación de personas para evitar la contaminación cruzada y la transmisión de enfermedades, daños en equipos y manipulación no adecuada de los recursos médicos disponibles.

Desde el punto de vista ingenieril, el control de acceso cuenta con una serie de retos y herramientas qué van a permitir desarrollar una base de datos para almacenar la información sobre las diferentes personas que acceden a un área, según el rol que desempeña la persona en el momento, también permite el uso de tecnologías basadas en el internet de las cosas que interactúan de una manera transparente (computación oblicua) con las personas permitiendo o restringiendo el acceso a ciertos espacios según los privilegios en el perfil de la persona y su rol.

Los sistemas de acceso deben ser fácilmente reprogramables y deben poder cambiar las configuraciones y restricciones a los diferentes perfiles y roles adaptándose en el menor tiempo posible, sin perder el historial generado sobre todos los accesos realizados por cada uno de los perfiles o roles, controlando e indicando incluso de ser posible el tiempo y tipo de acceso.

2. Materiales y métodos

2.1 Control de acceso basado en roles (RBAC)

Es una función de seguridad para controlar el acceso de usuarios a tareas que normalmente están restringidas al superusuario. Mediante la aplicación de atributos de seguridad a procesos y usuarios, RBAC puede dividir las capacidades de superusuario entre varios administradores. La gestión de derechos de procesos se implementa a través de privilegios. La gestión de derechos de usuarios se implementa a través de RBAC.[1], [2]

RBAC utiliza el principio de seguridad del privilegio mínimo. Privilegio mínimo significa que un usuario dispone exactamente de la cantidad de privilegios necesaria para realizar un trabajo. Los usuarios comunes tienen privilegios suficientes para utilizar sus aplicaciones, comprobar el estado de sus trabajos, imprimir archivos, crear archivos nuevos, etc. Las capacidades que van más allá de las capacidades de los usuarios comunes se agrupan en perfiles de derechos. Los usuarios que realizarán trabajos que requieren algunas de las capacidades de superusuario asumen un rol que incluye el perfil de derechos adecuado.[3]

RBAC recopila las capacidades de superusuario en perfiles de derechos. Estos perfiles de derechos se asignan a cuentas de usuario especiales denominadas roles. Luego, un usuario puede asumir un rol para realizar un trabajo que requiere algunas de las capacidades de superusuario.[4]

En el modelo RBAC, el superusuario crea uno o más roles. Los roles se basan en perfiles de derechos. El superusuario luego asigna los roles a los usuarios en los que confía para realizar las tareas del rol. Los usuarios inician sesión con su nombre de usuario. Después del inicio de sesión, los usuarios asumen roles que pueden ejecutar comandos administrativos restringidos y herramientas de la interfaz gráfica de usuario (GUI).

2.2 Identificación por radio frecuencia

La identificación automática, es un grupo de tecnologías, que se emplean para ayudar a que las máquinas identifiquen distintas personas. En general la ID Automática se asocia con la captura automática de datos, identificar personas, objetos, captar información acerca de los mismos y de alguna manera introducir esta información en un ordenador sin tener que recurrir a que tengan que hacerlo de forma manual.

La Identificación por radio frecuencia o RFID, es un término genérico que permite definir tecnologías que emplean ondas radiales para identificar de manera automática a personas u objetos.

Los componentes que participan en la tecnología RFID son cuatro: las etiquetas, los lectores, el software que procesa la información y los programadores.

Lector/ Escritor RFID: se encarga de recibir la información emitida por las etiquetas y transferirla al middleware o subsistema de procesamiento de datos. Las partes del lector son: antena, transceptor y decodificador. Algunos lectores incorporan un módulo programador que les permite escribir información en las etiquetas, si éstas permiten la escritura.[5]

Se desarrolló un prototipo lector de tarjetas RFID basado en el módulo Wi-Fi ESP8266 en su variante ESP12-E el cual se comunica con un módulo RFID RC522 por medio del protocolo SPI, el control de la apertura de las puertas se realiza mediante un relé que es operado por el módulo Wi-Fi ESP12-E que activa y desactiva un electroimán permitiendo así el cierre y la apertura de las puertas. El

lector se comunica con la aplicación Web mediante el protocolo MQTT.

Figura 1. Prototipo Lector RFID WiFi.

2.3 MQTT

Message Queuing Telemetry Transport (MQTT es un protocolo de mensajería basado en la publicación-suscripción TCP/IP sencillo y sumamente ligero. Se basa en el principio cliente/servidor.[6][7]

El servidor, llamado broker, recopila los datos que los publishers (los objetos comunicantes) le transmiten. Determinados datos recopilados por el broker se enviarán a determinados publishers que previamente así se lo hayan solicitado al broker.

El principio de intercambio se parece mucho al de Twitter. Los publishers envían los mensajes a un canal llamado topic. Los subscribers (suscriptores) pueden leer esos mensajes. Los topics (o canales de información) pueden estar distribuidos jerárquicamente de forma que se puedan seleccionar exactamente las informaciones que se desean.

Los mensajes enviados por los objetos comunicantes pueden ser de todo tipo pero no pueden superar los 256 Mb.[8]

2.4 Aplicación Web

Se desarrolló una aplicación web para el registro y control de los usuarios implementando los lenguajes de programación php , html5 , css3 y JavaScript. Los registros resultantes de las operaciones de ingreso y salida a las aéreas de la clínica son almacenados en una base de datos relacional PostgreSQL. El sistema de doble validación consiste en la implementación de un servicio web que comunica la aplicación principal con el hardware lector RFID-WiFi y una aplicación móvil para Smartphones Android y iOS a la cual es enviado un token numérico de 4 dígitos. Los usuarios que requieren acceso a zonas donde deben autenticarse mediante validación doble han de contar con una tarjeta RFID y la aplicación móvil instalada en un Smartphone en la cual deberán estar logeados para recibir el código de autenticación.

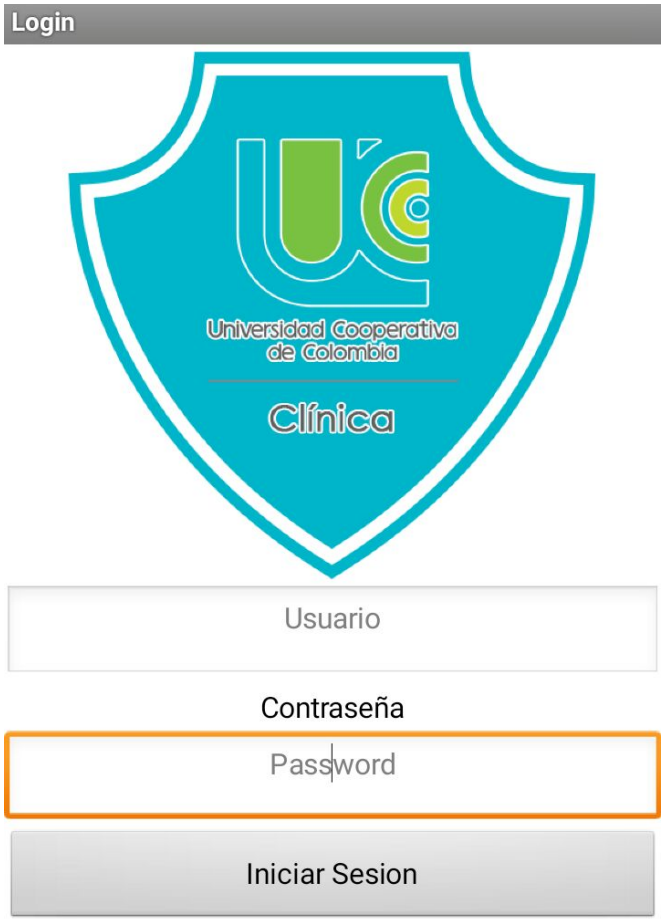

Figura 2. Login aplicación Smartphone.

2.4.1 Servicios web

El término "servicios web" designa una tecnología que permite que las aplicaciones se comuniquen en una forma que no depende de la plataforma ni del lenguaje de programación. Un servicio web es una interfaz de software que describe un conjunto de operaciones a las cuales se puede acceder por la red a través de mensajería XML estandarizada. Usa protocolos basados en el lenguaje XML con el objetivo de describir una operación para ejecutar o datos para intercambiar con otro servicio

web. Un grupo de servicios web que interactúa de esa forma define la aplicación de un servicio web específico en una arquitectura orientada a servicios (SOA)[9]

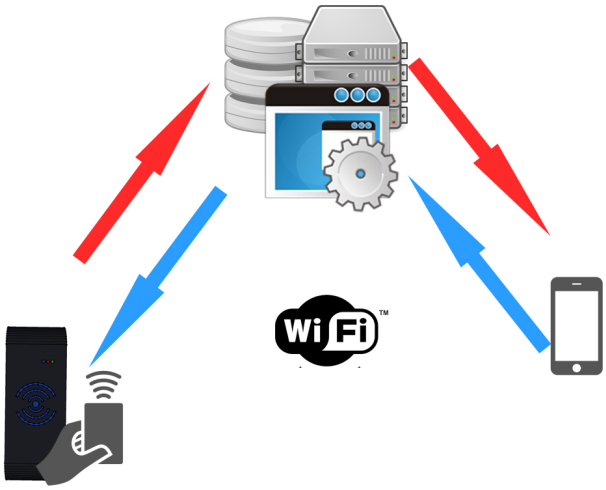

Figura 3. Arquitectura del Sistema. Fuente autores.

Figura 4. Pantalla de verificación de código.

2.5 SOAP y REST

SOAP es el acrónimo de "Simple Object Access Protocol" y es el protocolo que se oculta tras la tecnología que comúnmente denominamos "Web Services" o servicios web. SOAP es un protocolo extraordinariamente complejo pensado para dar soluciones a casi cualquier necesidad en lo que a comunicaciones se refiere, incluyendo aspectos avanzados de seguridad, transaccionalidad, mensajería asegurada y demás. Cuando salió SOAP se vivió una época dorada de los servicios web. Aunque las primeras implementaciones eran lo que se llamaban WS1.0 y no soportaban casi ningún escenario avanzado, todo el mundo pagaba el precio de usar SOAP, ya que parecía claro que era el estándar que dominaría el futuro. Con el tiempo salieron las especificaciones WS-* que daban soluciones avanzadas, pero a la vez que crecían las capacidades de SOAP, crecía su complejidad. Al final, los servicios web SOAP terminan siendo un monstruo con muchas capacidades pero que en la mayoría de los casos no necesitamos.[9], [10]

Por su parte REST es simple. REST no quiere dar soluciones para todo y por lo tanto no pagamos con una demasiada complejidad una potencia que quizá no vamos a necesitar.[11]

3. Conclusiones

- Actualmente en el mercado existen muchas herramientas, que cumplen con las tareas de un control de presencia, sin embargo no todas estas herramientas permiten la doble verificación.
- Para la implementación del control de acceso basado en roles RBAC, en forma fisica es necesario el compromiso participación y el respaldo de la alta gerencia.
- El uso de diferentes protocolos, en internet de las cosas como MQTT, permiten que los sistemas tengan estandares y se rigan por estos.

4. Referencias

[1]. E. Bertino, "RBAC models - Concepts and trends," Comput. Secur., vol. 22, no. 6, pp. 511–514, 2003.

[2]. S.-S. Tseng, H.-C. Chen, L.-L. Hu, and Y.-T. Lin, "CBR-based negotiation RBAC model for enhancing ubiquitous resources management," Int. J. Inf. Manage., vol. 37, no. 1, pp. 1539–1550, Feb. 2017.

[3]. S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the

Internet of Things," Math. Comput. Model., vol. 58, no. 5–6, pp. 1189–1205, Sep. 2013.
[4]. M. Giordano, G. Polese, G. Scanniello, and G. Tortora, "A system for visual role-based policy modelling," J. Vis. Lang. Comput., vol. 21, no. 1, pp. 41–64, 2010.
[5]. A. F. Márquez Arteaga, "DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO RFID EN MATERIALES METÁLICOS."
[6]. OASIS Standard, "MQTT Version 3.1.1," 2015.
[7]. K. Chooruang and P. Mangkalakeeree, "Wireless Heart Rate Monitoring System using MQTT," Procedia Comput. Sci., vol. 86, pp. 160–163, 2016.
[8]. S. Bonnet, "MQTT: un protocolo específico para el internet de las cosas | Digital Dimension," 2015. [Online]. Available: http://www.digitaldimension.solutions/es/blog-es/opinion-de-expertos/2015/02/mqtt-un-protocolo-especifico-para-el-internet-de-las-cosas/. [Accessed: 15-May-2017].
[9]. I. Ivanochko, M. Gregus, O. Urikova, and I. Alieksieiev, "Synergy of Services within SOA," Procedia Comput. Sci., vol. 58, no. Euspn, pp. 182–186, 2016.
[10]. "IBM developerWorks en español : Introducción a SOA y servicios web." [Online]. Available: https://www.ibm.com/developerworks/ssa/webservices/newto/service.html. [Accessed: 15-May-2017].
[11]. E. Tomàs, "Qué es REST," 2014. [Online]. Available: https://desarrolloweb.com/articulos/que-es-rest-caracteristicas-sistemas.html. [Accessed: 15-May-2017].