ARBOR Ciencia, Pensamiento y Cultura
Vol. 187 - Extra 3 - diciembre (2011) 135-151 ISSN: 0210-1963
doi: 10.3989/arbor.2011.Extra-3n3136

APLICACIONES Y SEGURIDAD EN LA IMPLEMENTACIÓN DE COMPETENCIAS PRÁCTICAS EN ENTORNOS DE GESTIÓN DEL APRENDIZAJE

APPLICATIONS AND SECURITY IN THE PRACTICAL COMPETITIVENESS IMPLEMENTATION WITHIN LEARNING ENVIRONMENTS

R. Gil, E. San Cristóbal, M. Tawfik, S. Martín, A. Pesquera, G. Díaz, A. Colmenar, J. Carpio, J. Peire y M. Castro

Departamento de Ingeniería Eléctrica, Electrónica y Control Industrial.
Universidad Nacional de Educación a Distancia-UNED
{rgil, elio, mtawfik, smartin}@ieec.uned.es
apm@innova.uned.es
{gdiaz, acolmenar, jcarpio, jpeire, mcastro}@ieec.uned.es

ABSTRACT: *In this article, some improvements and contributions are introduced into two main features of the Learning Management Systems (LMSs). The first feature is the security and the authentication functionality, where we present a model that combines the traditional authentication based on username and password, with the authentication based on fingerprints. The second feature is the access to remote and virtual laboratories, where we present a middleware architecture that combines the duplicated services provided by both, the laboratories and the LMS, in order to facilitate their integration and to provide a unique access from the LMS to the remote and virtual laboratories.*

KEY WORDS: *Authentication; distance education; biometric; fingerprint; remote laboratories; virtual laboratories; Learning Management System (LMS).*

RESUMEN: En este artículo exponemos algunas mejoras y aportaciones en dos aspectos de los sistemas de gestión de aprendizaje (LMS). El primer aspecto es la seguridad y la autenticación, donde presentamos una modalidad de combinar la autenticación tradicional de contraseña y nombre de usuario con la autenticación por la técnica biométrica de comparación de huellas dactilares. El segundo aspecto es una arquitectura middleware capaz de dar acceso desde los LMS a distintos laboratorios remotos y virtuales (online) de forma que, se evita la duplicación de los servicios proporcionados por ambas y se reutilizan los servicios proporcionados por los LMS en las sesiones prácticas.

PALABRAS CLAVE: Autenticación; educación a distancia; biometría; huella dactilar; laboratorios remotos; laboratorios virtuales; sistemas de gestión de aprendizaje.

1. Introducción

La educación a distancia es tanto una causa como un resultado de los cambios significativos de cómo entendemos la educación por sí misma y como se entiende que debería organizarse. Como primera apreciación se puede ver que la educación a distancia llega a más personas con mayor facilidad y mayor calidad de recursos que en el pasado. Los cursos se pueden recibir desde cualquier localización en el mundo. Más allá del acceso, la educación a distancia da un mayor grado de control a los estudiantes en relación con el centro de enseñanza. Para preparar un curso a distancia no sólo se necesita de expertos de contenido sino también diseñadores que puedan organizar el contenido acorde a lo que ya se sabe y como se quiere alcanzar un nuevo conocimiento. Por tanto el concepto de educación a distancia tiene más de una implicación que se debe tratar. En este artículo, tan sólo nos centramos en los aspectos que conciernen a la seguridad y a las prácticas en entornos de Gestión del Aprendizaje. En nuestro caso particular, Moodle.

La biometría como técnica diseñada para la seguridad tiene como principal objetivo discriminar a un individuo de un grupo sobre alguna muestra previamente almacenada de él mismo, es decir identificar o verificar la identidad

que reclama. Hasta ahora la aplicación por excelencia de la biometría ha sido los controles de acceso a edificios físicos, pero frente a la aparición de nuevas opciones en la red, como pagos o trasferencias bancarias, cobra sentido aplicar la biometría a campos de control de redes. El concepto de biometría aplicado a la enseñanza a distancia puede ser relativamente nuevo y su justificación parte de la idea de que uno de los procesos relacionados con el aprendizaje – la evaluación–, sea auténtica, y proporcione credibilidad a la calidad de los cursos a distancia. Las oportunidades de la biometría están limitadas hoy en día al tiempo de su estudio y elaboración, también a posibles limitaciones tecnológicas y al factor determinante de la sociedad. Es irremediable asociar biometría a algo intrusivo, a algo con connotaciones criminales. El objetivo será convertir estos problemas en soluciones o recursos. Integrar sensores en los recursos que utilice un estudiante, puede además de verificar una identidad, dar recursos o información única que interese a ese individuo en particular. De forma, que da igual desde que terminal acceda, con la rapidez de un contacto táctil, visual o de otra forma se podrá presentar información útil al individuo. Por supuesto una información específica a un usuario se podría dar igualmente a través de un nombre de usuario y contraseña. La biometría tendrá sentido en el grado que se busque una inmediatez de acceso sin ningún paso de identificación previo, y cuando los recursos a los que se acceden son de un relevante valor en el aprendizaje, en pérdidas económicas o en seguridad de instalaciones.

Los laboratorios virtuales permiten al alumno realizar experimentos basados en una simulación de los instrumentos reales, mientras que los laboratorios remotos son laboratorios reales manejados remotamente (online). Los laboratorios remotos y virtuales tienen su propia interfaz que contiene los servicios administrativos del laboratorio pero al mismo tiempo, carecen de muchos de los servicios que proporcionan LMS y que puedan ser necesarios para la gestión de las sesiones prácticas dentro del curso.

En este artículo se presentan dos módulos desarrollados por el Departamento de Ingeniería Eléctrica, Electrónica y Control Industrial de la Universidad Nacional de Educación a Distancia (UNED) e integrados con los LMS de código abierto (Moodle). Uno es para autenticación por huellas dactilares y el segundo es para la agregación de laboratorios online comunicando con ellos a través de una capa middleware que combina los servicios comunes proporcionados por los sistemas de gestión de aprendizaje y los laboratorios online para evitar la duplicación de los servicios (ej., Doble autenticación). Lo cual daría lugar a la reutilización de los servicios proporcionados por los sistemas de gestión de aprendizaje en los laboratorios y viceversa.

2. Sistemas de Gestión de Aprendizaje (LMS)

Un sistema de gestión de aprendizaje es una plataforma online utilizada por el profesor para la gestión y la administración de los cursos educativos y de los objetos de aprendizaje, asimismo, se utiliza por el alumno para realizar sus cursos online. Los LMS proporcionan muchos servicios y herramientas como:

Administración y gestión. Registro, perfiles de usuarios, asignación de tutores, alumnos y grupos, facturación, organización del contenido de los cursos, reservas, autenticación, etc.
Comunicación síncrona y asíncrona. Chat, foros, webinar, video conferencia, eventos, noticias, correo electrónico, calendarios, blog, etc.
Compartición de multimedia. Subir y bajar videos, audios, fotos, ficheros, etc.
Evaluación. Encuestas, exámenes, tareas, etc.
Compatibilidad. Los LMS organizan los objetos de aprendizaje en una estructura jerárquica según un estándar interoperable con el fin de permitir la importación y la migración de los contenidos entre los distintos tipos de LMS sin tener que volver a organizarlos de nuevo. Entre los estándares más utilizados se encuentran: SCORM y IMS para empaquetar contenidos, IMS-QTI para creación y reutilización de pruebas de evaluación y LOM y Dublin Core para descripción de los objetos de aprendizaje (metadatos).

Los LMS pueden ser de código abierto como: Moodle, Dot-LRN, Sakai, Caroline, etc. Los cual permiten modificaciones. Por tanto, se focaliza en este tipo a la hora de realizar una investigación o desarrollo, y en nuestro caso particular Moodle. Mientras el otro tipo de los LMS es propietario como: Blackboard, JoomlaLMS, SharePointLMS, etc. Solo puede ser desarrollado o modificado por el dueño. Los LMS

ARBOR Vol. 187 Extra 3 diciembre [2011] 135-151 ISSN: 0210-1963 doi: 10.3989/arbor.2011.Extra-3n3136

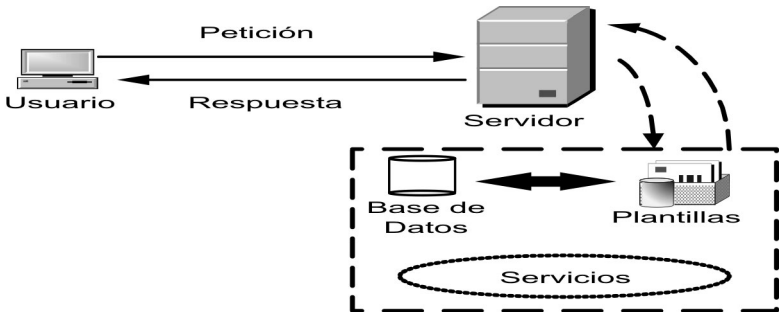

Figura 1. Arquitectura básica de un sistema de gestión de aprendizaje.

no se limitan en el aprendizaje teórico, sin embargo, son comúnmente utilizados para tal fin. La arquitectura de un LMS (Figura 1), está dividida en varios elementos: una base de datos, unos servicios (módulos, bloques, paquetes, etc.) y un servidor Web.

3. Autenticación por Huella Dactilar en Moodle

La Figura 2 muestra el diagrama de funcionamiento interno del sensor que se utilizó en la integración con el sistema de gestión de aprendizaje Moodle. La huella dactilar tiene una serie de características globales o locales que nos permiten diferenciar sujetos. Como características globales están: el core, el cual es el punto central donde las crestas cambian de dirección bruscamente retornando; y la delta, es el punto más próximo al centro geométrico donde tiene lugar la divergencia de las crestas de referencia, las cuales delimitan el área de interés o de estudio de la huella. Las características locales son los puntos donde se producen discontinuidades en el patrón de crestas, lo que recibe el nombre de minucias. Dentro de la clasificación de distintas minucias las más importantes son las bifurcaciones de crestas y los finales de crestas.

El proceso de comparación de huellas sigue un proceso previo de mejora de imagen donde se elimina ruido de la huella y se realiza un filtro paso banda mediante filtros Gabor los cuales son selectivos a la frecuencia y orientación local. Al realizar una comparación por minucias se convierte la imagen de escala de grises a binaria, se adelgaza el grosor de las líneas a 1 pixel y se extraen las minucias mediante un escaneo de ventana 3×3 a todos los vecinos cercanos a un pixel buscando una bifurcación o un final de línea. Dentro de los algoritmos de comparación se pueden distinguir tres técnicas importantes, de las cuales surgen variantes: técnicas basadas en correlación cruzada, en *fingercode* y en minucias. La técnica de minucias que es la que se emplea en este caso, es la que mejor resultados se obtienen en imágenes de media calidad, aunque tiene el mayor tiempo de cómputo. Para baja resolución es preferible usar correlación cruzada ya que la comparación se realiza con toda la huella entera. Para la comparación de minucias se debe realizar una translación y rotación de las huellas que se comparan a partir de un punto de referencia entre ambas, seguidamente se compara la similitud entre las minucias extraídas en ambas.

La aplicación que se desarrolló en esta investigación, tenía como finalidad combinar los sistemas tradicionales de autenticación, es decir los basados por nombre de usuario y contraseña con la huella dactilar de cada sujeto, por tanto la comparación que se realiza será 1:1, tratándose de una verificación del usuario que presenta unos datos (nombre de usuario y contraseña) con su verdadera identidad. Por tanto en la base de datos deberá estar previamente almacenada una huella dactilar, esta se almacenará en el momento de registrarse en el sitio de Moodle y será un dato que se pedirá cada vez que accedamos al sitio de Moodle.

Moodle está implementado para el uso de Apache, MySQL y PHP, lo cual se conoce como plataforma LAMP. Aunque también se puede hacer uso de otras bases de datos como PostgreSQL. Cuando se instala Moodle da lugar a una

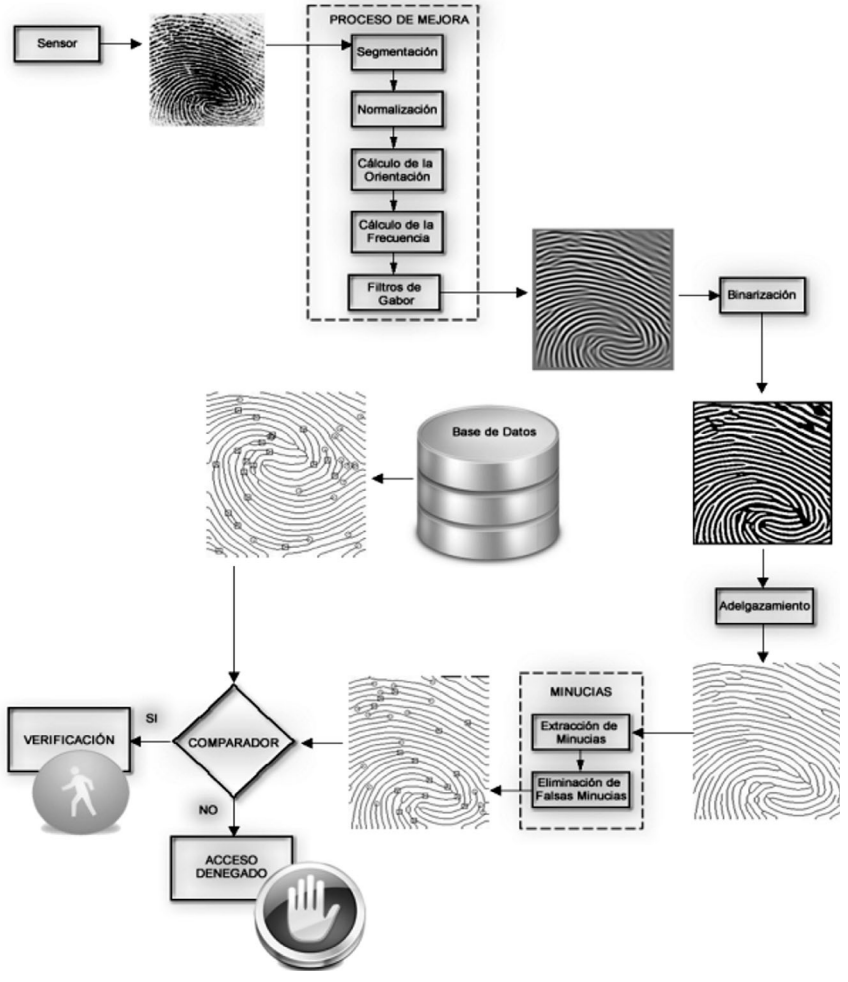

Figura 2. Diagrama de funcionamiento de comparación de huellas por minucias.

serie de archivos y carpetas. En orden de integrar la verificación por huella dactilar en el acceso a nuestro sitio de Moodle se deberá modificar alguna de estas carpetas. Principalmente se modificará la carpeta *login/* donde habrá que introducir nuevos elementos en el acceso al sitio de Moodle, este nuevo elemento será la solicitud de la huella dactilar, esto dará lugar a añadir nuevos elementos en la base de datos de Moodle que gestiona la información de los usuarios, **mdl_user.** También destacar que se debe modificar la carpeta *mod/* que contiene todos los módulos generales (fórum, chat, etc.), con vistas a añadir otra actividad no contemplada en el paquete estándar de Moodle y que nos sirva para evaluar la aplicación de integrar la verificación por huella dactilar en Moodle, o mejor dicho que sean los estudiantes los que evalúen a través de un cuestionario la eficacia de esta integración.

La versión actual que ofrece Moodle para autenticarse comprende: Autenticarse vía email; por cuentas manuales; sin autenticarse; PAM *(Pluggable Authentication Modules)*; Shibboleth; un servidor CAS (SSO); un servidor POP3; y un servidor LDAP. Por tanto la página de entrada o *login* será diferente según la opción que se elija. Incluso se puede añadir un enlace externo para que la autenticación se realice de otra forma alternativa. Además se puede visualizar o no la opción de entrar al sitio de Moodle por el rol de

ARBOR Vol. 187 Extra 3 diciembre [2011] 135-151 ISSN: 0210-1963 doi: 10.3989/arbor.2011.Extra-3n3136

Invitado o no, este botón se puede ocultar. Como buena política de seguridad se debe evaluar la conveniencia de que exista este rol o no, desde luego un Invitado tendrá permisos muy limitados, se le suele proporcionar la capacidad de leer total o parcialmente el sitio. Como medio para que estudiantes se apunten a un curso después de leer sus características podría ser muy útil mantener activo este botón.

En nuestra aplicación se realizó una autenticación vía email. Esta es la forma predeterminada en la que funciona Moodle. El usuario libremente escoge un nombre de usuario y contraseña y queda pendiente de un email de confirmación. Se le envía un email al usuario con un enlace seguro donde deberá confirma su cuenta. Hasta que no se confirme no se podrá acceder. En la base de datos de Moodle en MySQL, la tabla **mdl_user** posee un campo etiquetado con *confirmed,* el cual se mantiene en cero hasta que se confirme el enlace cambiándolo a uno. La aplicación propuesta es integrar el reconocimiento de huella dactilar como un dato más tanto en la fase de darse de alta o registrarse en el sitio como cada vez que se acceda al sitio con una cuenta, por tanto se deberá introducir cambios en los archivos que gestionan el *login* al sitio de Moodle. La carpeta *login/* está compuesta por los siguientes archivos (Tabla 1).

Esta aplicación tendrá dos situaciones: registrarse como estudiante y estudiantes ya inscritos. Por tanto habrá dos bloques de archivos que se deberán modificar:

- *signup.php* y *signup_form.php* - Registrarse como estudiante (Figura 3)
- *index.php* e *index_form.html* - Estudiantes ya inscritos (Figura 4)

Además se modificaron otros archivos de otras carpetas de *moodle/* que están relacionadas con estos archivos. La implicación de tomar un dato nuevo para el registro o acceso al sitio de Moodle, trae consigo que debe existir un dato de referencia en una base de datos con el que comparar el nuevo dato. Por tanto a la hora de registrarse en el sitio de Moodle como estudiante pedirá la huella dactilar la cual será la referencia de comparación en los sucesivos accesos al sitio de Moodle. La base de datos no es externa a Moodle sino que se optó por añadir un nuevo campo en la tabla de la base de datos que Moodle usa para acceder o registrarse en el sitio de Moodle que es **mdl_user.** Esto implica que también se modificó esta tabla de Moodle.

En ambos diagramas aparece un módulo NBioBSP COM que hace uso de las librerías que ofrece el sensor biomé-

TABLA 1: ARCHIVOS EN LA CARPETA LOGIN/

Nombre	Descripción
change_password.php y change_password_form.php	Página para cambiar la contraseña
confirm.php	Para confirmación de entrada a un sitio
environment.php	Para configurar variables en la sesión actual
forgot_password.php y forgot_password_form.php	Página para recuperar una contraseña olvidada
index.php e index_form.html	Página principal para entrar al sitio que muestra las opciones:
	• Estudiantes inscritos
	• Registrarse como estudiante
logout.php	Archivo para finalizar una sesión
mnet_email.php	Gestión de emails
restored_password_form.php	Fichero para realizar una solicitud a *forgot_password.php*
signup.php y signup_form.php	Página para registrar nuevos estudiantes

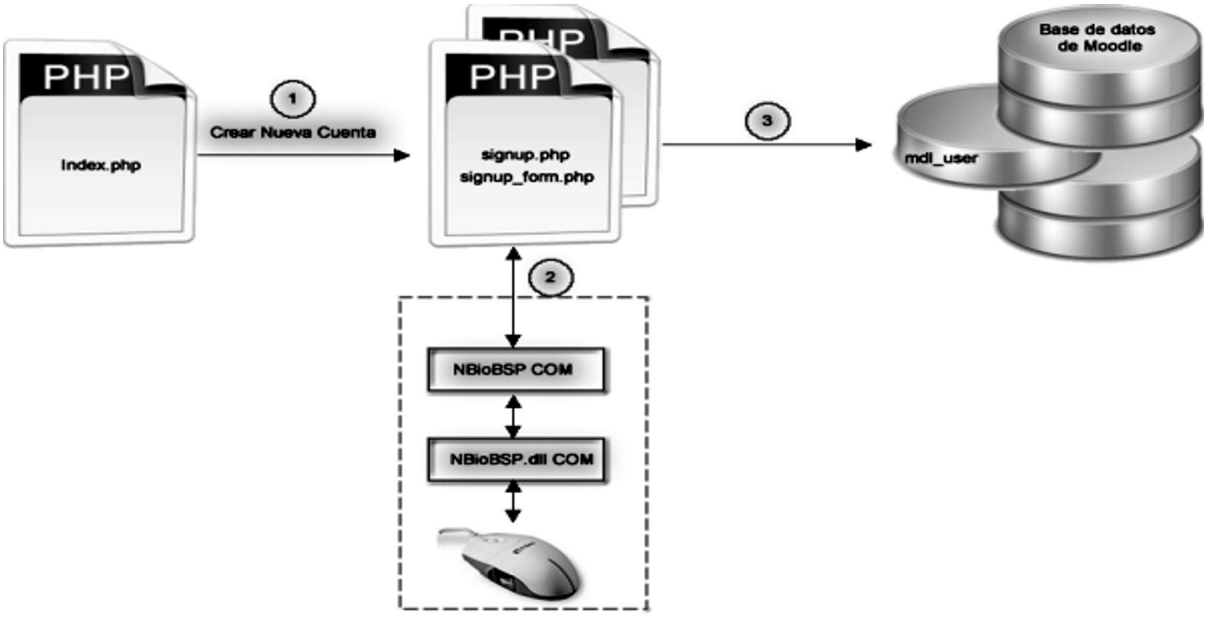

Figura 3. Diagrama en el registro de un nuevo estudiante.

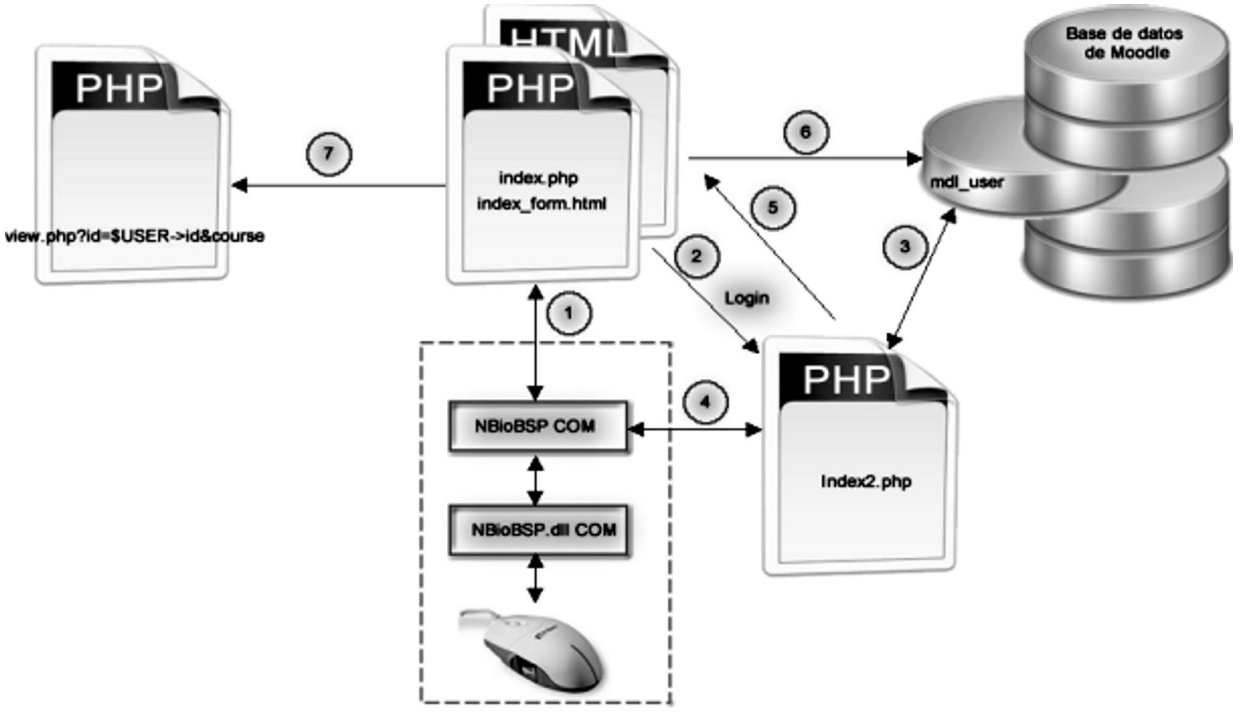

Figura 4. Diagrama de acceso a nuestro sitio de Moodle para usuarios ya registrados.

ARBOR Vol. 187 Extra 3 diciembre [2011] 135-151 ISSN: 0210-1963 doi: 10.3989/arbor.2011.Extra-3n3136

trico que se presenta en un ratón biométrico y se usan para los procesos de registro y verificación. Se programó en PHP con Javascript, lo cual hace posible introducir líneas de código en los archivos originales de Moodle.

La página de inicio de un sitio de Moodle, en nuestro caso se ha llamado **moodlab,** viene definida en *index.php.* La pantalla se divide en dos columnas principales: para acceder a **moodlab** y para entrar por primera vez. Al hacer click en el botón de "Crear nueva cuenta" nos remitirá a la página *signup.php,* la cual es un formulario de inscripción. Los campos y funcionamiento de este archivo vendrán definidos por *signup_form.php* que será el archivo que modificaremos.

Para empezar, en el archivo *signup_form.php* se debe definir el módulo NBioBSP COM para que todas las funciones asociadas se reconozcan. Para realizar esto, nuestro archivo PHP se convertirá en un archivo HTML con PHP y Javascript. Antes de definir la cabecera <head> del archivo, se declara el módulo como un objeto. El cuerpo del archivo será el archivo PHP original con un campo nuevo en el formulario para la casilla de la huella dactilar que se etiquetará como **FPText.** Este campo se le asignará como atributo que sea "requerido", es decir que al enviar los datos del formulario se deberá cumplimentar esta casilla para poder completar el registro. Se ha definido esta casilla para que cuando se posicione el ratón en ella se acceda a la función **pregunta( )** definida en la cabecera de este archivo como Javascript. En la función **pregunta( )** se implementa las llamadas al ratón, para capturar y obtener una plantilla de una huella dactilar.

En el archivo *signup_form.php* se verifica que los datos son correctos como que no haya un mismo usuario con el mismo nombre de usuario o contraseña por ejemplo. Los datos se almacenan en la tabla de Moodle **mdl_user.** Al añadir la huella dactilar se debe añadir un nuevo campo en esta tabla para almacenarla, se tratará en formato texto como una cadena de caracteres codificada a 128-bit tipo MD5, por lo tanto se debe añadir un *longtext* en la tabla. En la Figura 5 se muestran el nuevo formulario que se ha creado con el campo **Fingerprint capture.**

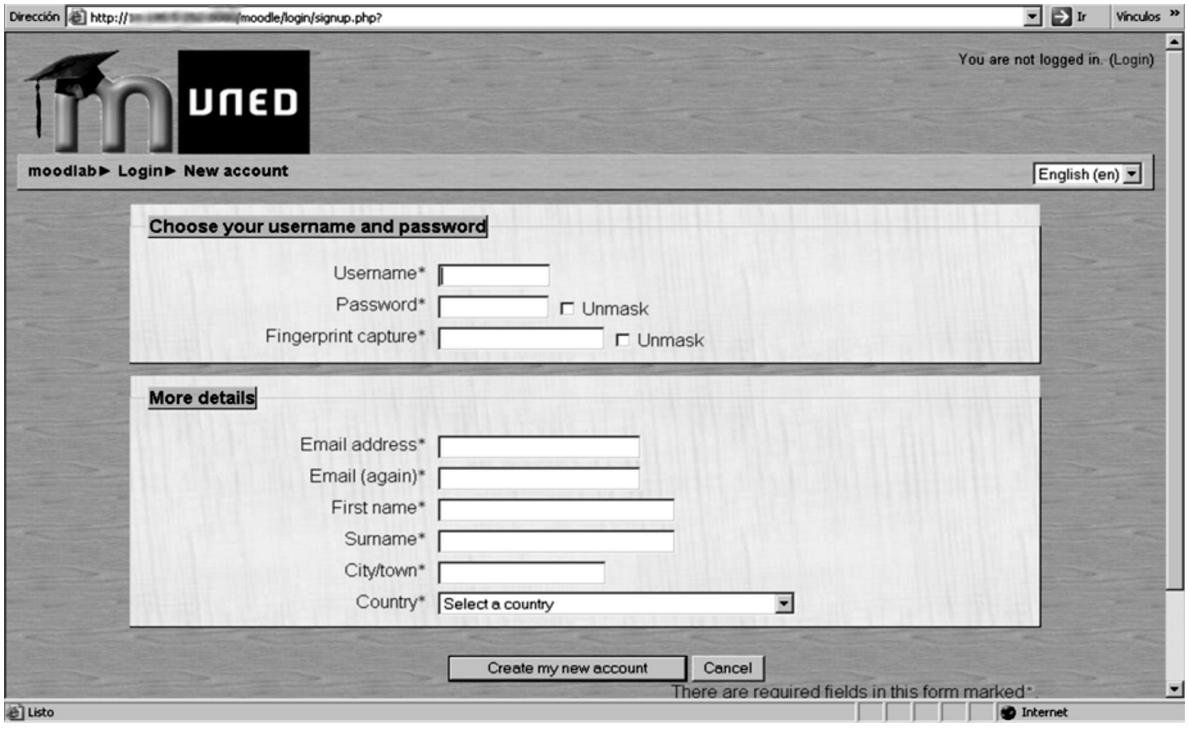

Figura 5. Nuevo formulario para registrarse como usuario en moodlab.

doi: 10.3989/arbor.2011.Extra-3n3136 ARBOR Vol. 187 Extra 3 diciembre [2011] 135-151 ISSN: 0210-1963

En el caso que el usuario ya posea un nombre de usuario y contraseña válidos y almacenados en la tabla **mdl_user** de Moodle. Al acceder a la página de inicio *index.php* se muestran dos opciones: acceder como estudiante ya inscrito y registrarse como nuevo estudiante. Los datos que se verificarán serán el nombre de usuario y la contraseña como se venía haciendo y además la huella dactilar. Para este último campo se añadirá un nuevo campo en el formulario de acceso al sitio, que será la huella dactilar **(Fingerprint)**, por tanto se capturará una nueva huella dactilar cada vez que alguien quiera acceder y se comparará esta nueva muestra con la ya almacenada en la tabla **mdl_user** en el campo **FPText** para ese usuario, el cual posee un nombre de usuario y contraseña únicos.

Primero se accede a la página de inicio de nuestro sitio de Moodle *(index.php)*. Se modifica el archivo *index_form.html* de tal forma que incluya un campo nuevo en el formulario que será la Huella dactilar. Las modificaciones serán:

- Se declara NBioBSP COM como un objeto del archivo de tal forma que las funciones que se utilicen de la librería se reconozcan.
- Mediante **onfocus( )** se ejecutará el Javascript **(pregunta( ))** que se programó y se capturará una nueva huella dactilar **FPTextNow** que servirá para compararla con la almacenada en la base de datos más adelante.
- Se modificará el formulario de forma que cuando se pulse el botón de **Login** se acceda a *index2.php* y no a *index.php* como ocurría originalmente.

El archivo *index2.php* se ha creado nuevo para poder acceder a la tabla **mdl_user** y comparar la nueva huella dactilar **FPTextNow** con la huella almacenada basándonos en el nombre de usuario. En caso de que la verificación sea correcta se accederá a *index.php* y en caso contrario se accederá también a *index.php* pero con todos los campos vacios, es decir se tendrá que volver a rellenar el formulario, lo que implica volver a ingresar una nueva huella dactilar para compararla junto con una nueva contraseña y nombre de usuario.

En el caso de que la comparación fuera correcta, es decir que se ha verificado la identidad de ese usuario mediante la huella, *index2.php* remite a *index.php.* Este último archivo realiza las verificaciones propias y por defecto de Moodle respecto al nombre de usuario y contraseña, en caso que se verifique esta última comparación el archivo *index.php* nos remitirá a la página principal de los cursos que estén asociados para ese usuario *(course/view.php?id=)*. La Figura 6 muestra la página de inicio *(index.php)* con el nuevo campo del formulario introducido en *index_form.html* para la huella dactilar.

Note que al remitir a *index.php* para terminar con la verificación de datos es inapreciable en el proceso de acceder por parte del usuario, una vez que escribe sus datos e introduce una huella dactilar es prácticamente inmediato la visualización de la página principal de nuestros cursos Gil (2010).

4. Laboratorios Remotos y Virtuales

Los laboratorios remotos y virtuales permiten la adquisición de las habilidades prácticas y la experimentación a distancia (online) o bien por una simulación o bien por un manejo a distancia de los instrumentos reales. Los laboratorios virtuales son laboratorios simulados en forma de un software o bien ejecutable desde el ordenador o bien incrustados en una página web (online). Suelen ser desarrollados por tecnologías de animación como Java Applets, Adobe Flash, Microsoft Silverlight, etc. O con otros programas como Matlab, Pscpice, LabVIEW, etc. Son laboratorios más seguros y no presentan ningún tipo de riesgo, ya que no se trabaja con instrumentos reales. Por tanto, no exigen sistemas de seguridad, reservas, administración, control de acceso, etc. Su única desventaja es que no pueden predecir con exactitud el rendimiento de los instrumentos reales. Los laboratorios remotos son laboratorios reales manejados por internet. Suelen ser accesibles por un interfaz web, que lleva el proceso de gestión y administración del laboratorio, conectado a un controlador que maneja el control de los instrumentos reales. La Figura 7 explica la estructura común de un laboratorio remoto. A continuación se detalla brevemente los componentes principales de esta estructura.

Web Interfaz. Es el sitio web que lleva la gestión y la administración del laboratorio (registro, autenticación, banco de trabajo remoto). Se desarrolla por lenguajes de programación web (HTML, JavaScript, PHP, ASP.NET, etc.) más

ARBOR Vol. 187 Extra 3 diciembre [2011] 135-151 ISSN: 0210-1963 doi: 10.3989/arbor.2011.Extra-3n3136

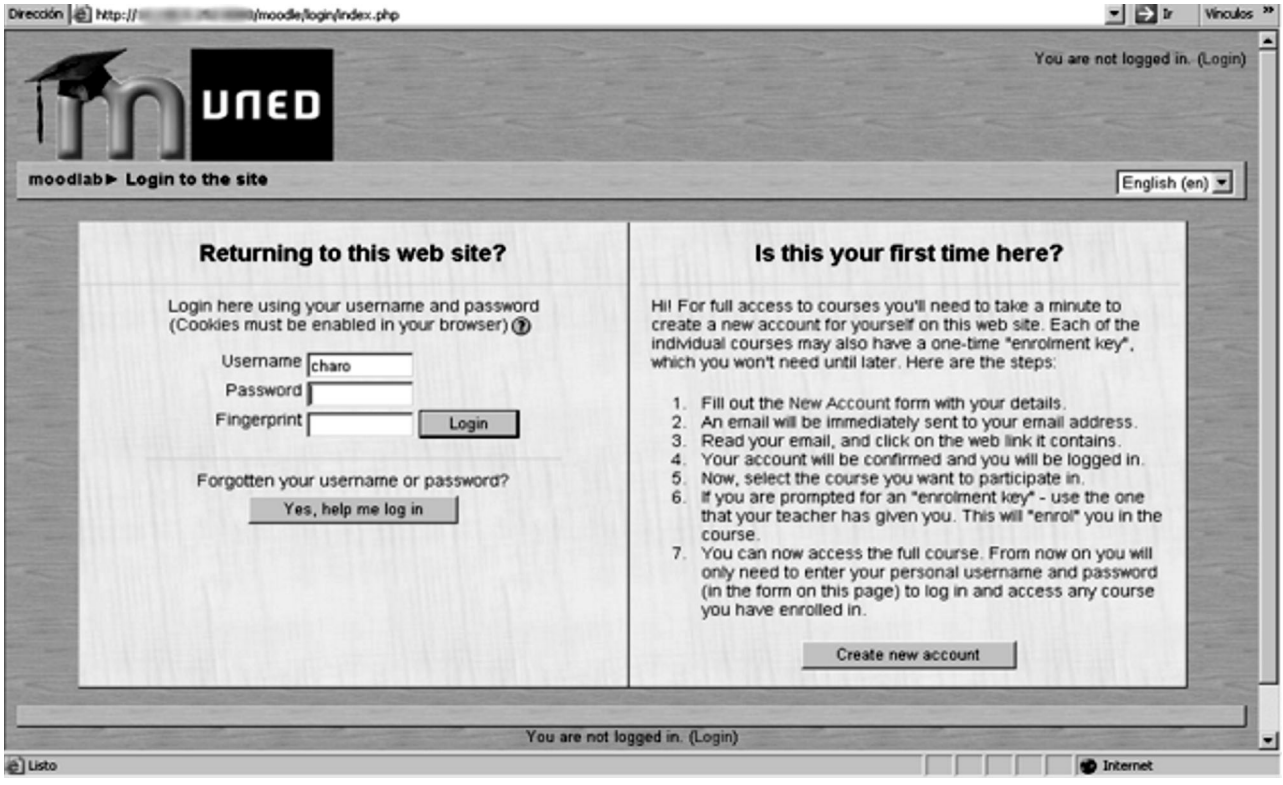

Figura 6. Página de inicio (index.php).

otras tecnologías web como animación Flash, Silverlight, Java Applets, etc.

Servidor Web. Es el servidor que aloja el sitio web (ej. Apache, IIS, etc.). Se conecta a una base de datos (MySQL, MS SQL, Oracle, etc.) para el almacenamiento de los datos de los usuarios. Una vez el servidor web autentique al usuario, el usuario se conecta al servidor del laboratorio para controlar los instrumentos.

Servidor del laboratorio. Es una aplicación web desarrollada por un lenguaje de control y automatización como LabVIEW, C#, C/C++, VHDL, etc. Se encarga de interpretar la petición recibida del usuario, por protocolos de comunicación como TCP/IP o servicios web, a señales comprensibles por el controlador de los instrumentos. Asimismo, puede ser una plataforma en la cual el usuario programa al controlador.

Controlador. Es un dispositivo electrónico (Ej. Micro-controlador, Controlador Lógico Programable (PLC), etc.). Programado por el servidor del laboratorio que controla de forma directa los instrumentos reales.

Convertidor. Actúa como un interruptor o un enchufe (Ej. Conversión analógica-digital) para la conexión directa de los instrumentos reales con el controlador. Se elige dependiendo de las características de las salidas y las entradas de los instrumentos y los controladores.

Instrumentos adicionales. Son instrumentos complementarios para el control remoto de un laboratorio. Por ejemplo, una cámara web para notar el rendimiento de los instrumentos a distancia. Pueden ser controlados directamente por el servidor del laboratorio o por el controlador.

Muchas universidades e instituciones tienen sus propios laboratorios remotos y virtuales (online) desarrollados con distintas tecnologías. Cada laboratorio tiene su propio interfaz de acceso y sistema de administración. La arquitectura Com-

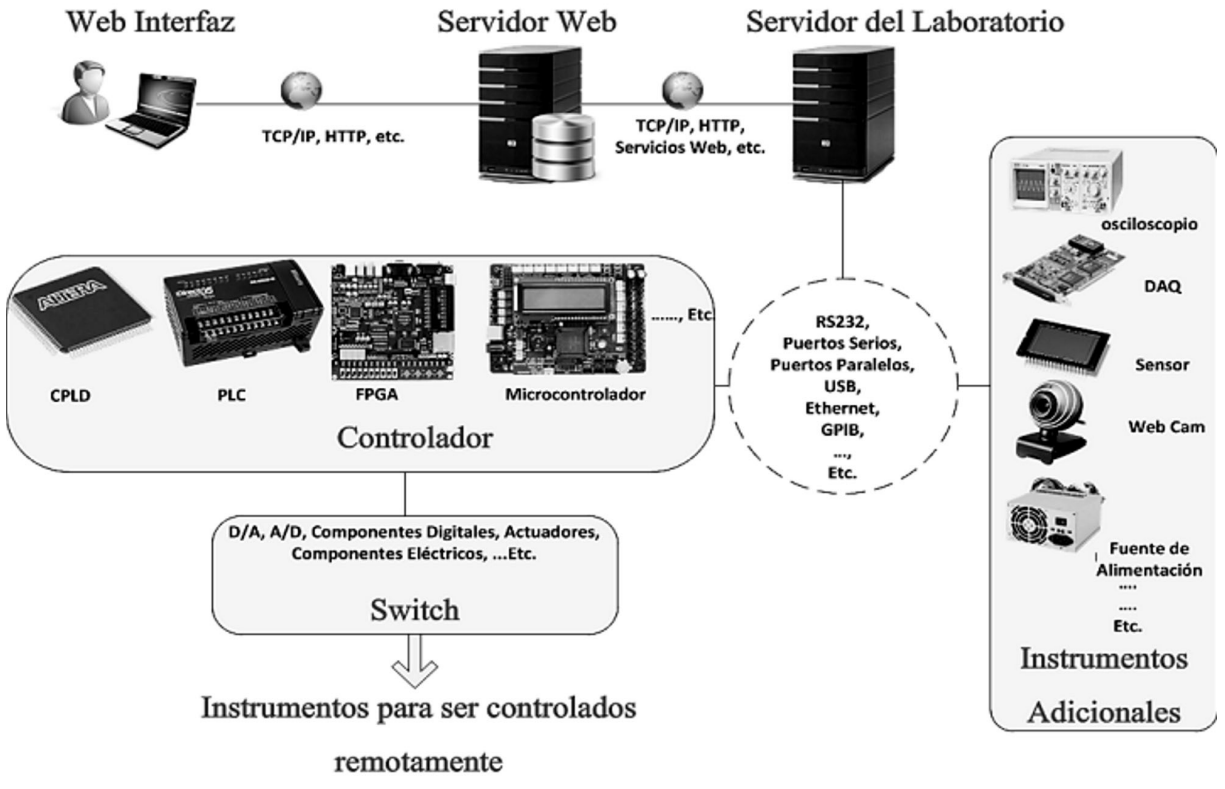

Figura 7. Estructura común de un laboratorio remoto.

partida de iLab (ISA), Harward (2008), ha conseguido unificar los servicios comunes de administración proporcionados por todos los laboratorios online. Es una infraestructura basada en servicios web y fue desarrollada por el Instituto de Tecnología de Massachusetts (MIT) con fin de crear una plataforma única capaz de proporcionar acceso a una variedad de laboratorios online heterogéneos y comunicarse con ellos. Se trata de un servidor broker instalado en la universidad de los usuarios que se comunica con los servidores de distintos laboratorios de otras universidades con los servicios web y conlleva todo el proceso de administración.

5. Arquitectura Middleware

Muchos servicios proporcionados por los LMS pueden ser útiles y beneficiosos para las sesiones prácticas como: herramientas de comunicación, agrupación, evaluación, tareas, etc. Además, existen muchos servicios comunes proporcionados por los LMS y los Laboratorios online como: autenticación, reservas, etc. Estos servicios podrían ser unidos para evitar esfuerzos adicionales y conseguir una plataforma educativa completa. Desafortunadamente, no existe ninguna arquitectura que revela una relación directa entre los laboratorios online y los LMS. La arquitectura compartida de iLab (ISA) es una iniciativa brillante para unificar el acceso y la administración de distintos tipos de laboratorios online, no obstante, no contempla los LMS ni la reutilización de los servicios proporcionados por ellos. Por estas razones, el Departamento de Ingeniería, Eléctrica, Electrónica y Control Industrial de la UNED decidió crear una arquitectura middleware capaz de integrar los laboratorios online con los LMS para reutilizar los servicios proporcionados por ambas. La Figura 8 muestra la situación actual de los laboratorios online y los LMS, cada uno de

ARBOR Vol. 187 Extra 3 diciembre [2011] 135-151 ISSN: 0210-1963 doi: 10.3989/arbor.2011.Extra-3n3136

ellos proporciona sus propios servicios y algunos de ellos son comunes en ambas. La Figura 9 muestra el fin de la integración y la creación de dicha arquitectura, San Cristóbal (2010).

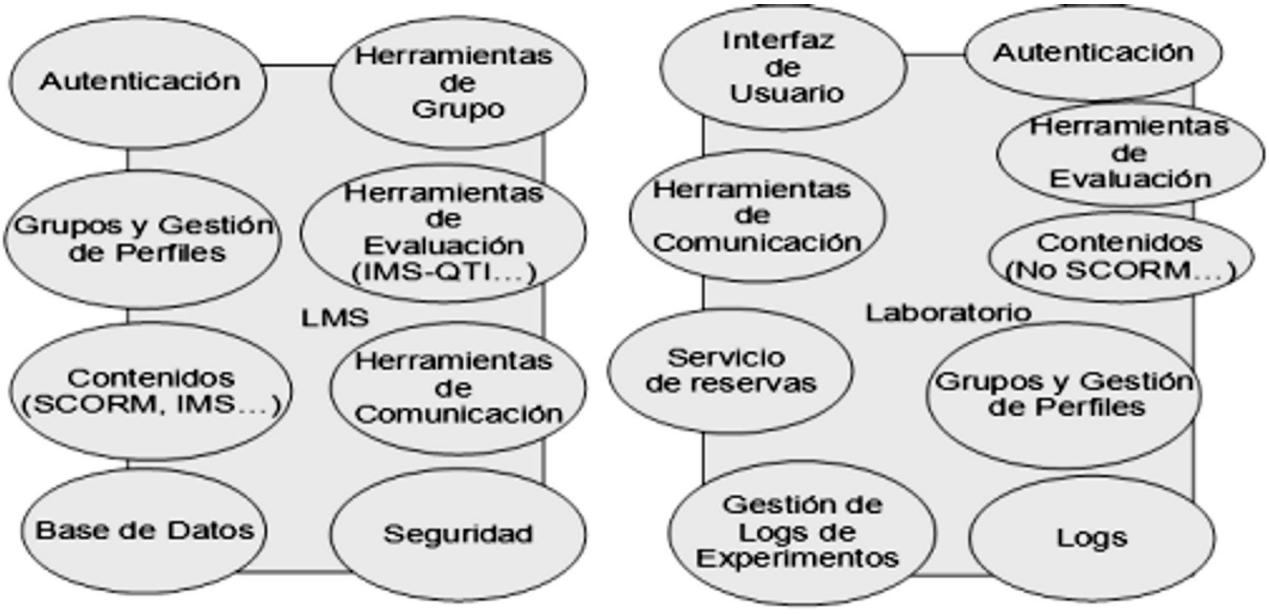

Figura 8. Situación actual de los laboratorios online y los LMS.

Figura 9. Integración de los servicios de los laboratorios online y los LMS.

La arquitectura middleware es una arquitectura basada en servicios web que permite el acceso desde los LMS a varios laboratorios online heterogéneos o a la arquitectura compartida de ilab (ISA), asimismo, evita la duplicación de los servicios y permite la reutilización de los servicios proporcionados por LMS en las sesiones prácticas (Figura 10).

Para lograr este tipo de integración, es necesario establecer una arquitectura capaz de comunicarse a través de todos los sistemas heterogéneos. Una de las mejores soluciones disponibles hoy en día, es la arquitectura Orientada a Servicios de cliente SOA. SOA es la base para implementar los servicios web (SOAP, REST, etc.) a través

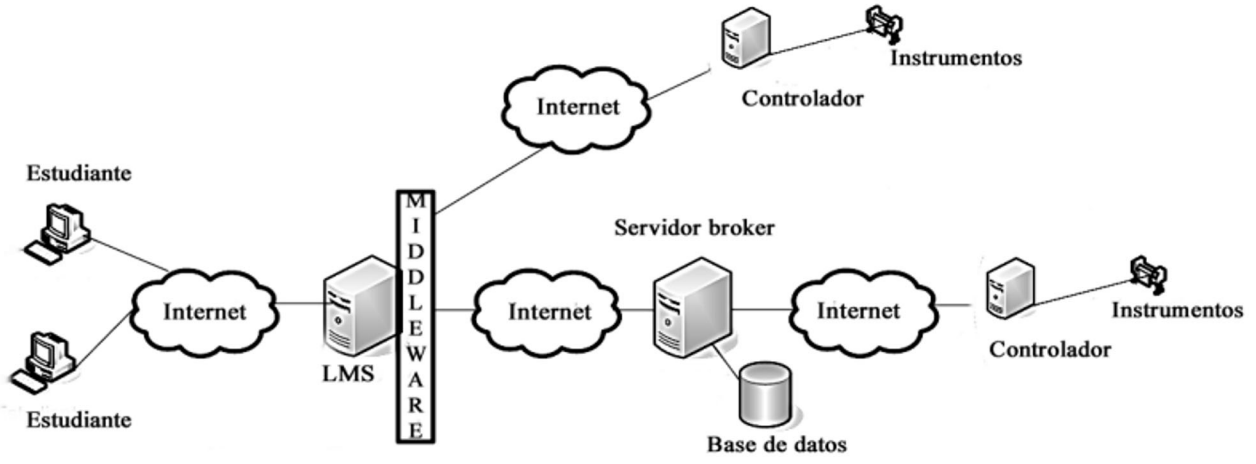

Figura 10. Arquitectura Middleware.

de múltiples sistemas distribuidos con el objetivo de conseguir flexibilidad, escalabilidad y tolerancia a fallos. SOA no está ligada a una tecnología en concreto, pero si se utilizan las tecnologías existentes para desarrollarla. Con el uso de las especificaciones de los servicios web, SOA permite que los sistemas heterogéneos puedan buscar, encontrar y utilizar el servicio que necesitan independientemente del sistema que lo ofrece y el cliente que lo consume.

La Figura 11 muestra la implementación de la arquitectura SOA con el protocolo de los servicios web SOAP. SOAP es un protocolo basado en XML para el intercambio de datos estructurados implementados en servicios web. Para ello, se necesita el protocolo WSDL que proporciona un modelo para la descripción de los servicios web en un formato XML. El cliente utiliza SOAP para llamar a una de las operaciones listadas en WSDL. Además, se necesita el protocolo UDDI que actúa como un repositorio de todos los servicios web listados en WSDL y llamados por SOAP.

SOA permite la reutilización de servicios, eso sí, tanto el cliente como el servicio deben utilizar la misma arquitectura (REST, SOAP) y dentro de ellos ser capaces de entender tanto las peticiones como las respuestas a esas peticiones.

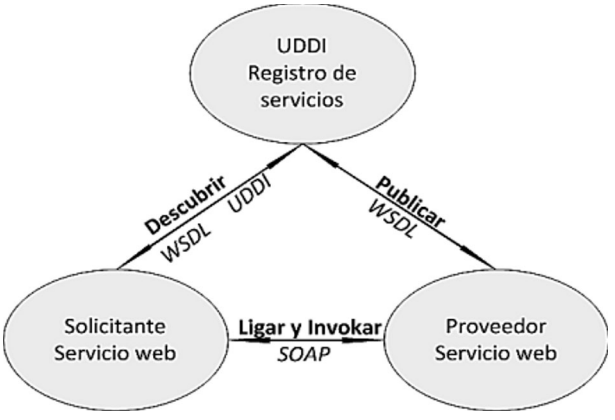

Figura 11. Implementación de la Arquitectura SOA con SOAP.

ARBOR Vol. 187 Extra 3 diciembre [2011] 135-151 ISSN: 0210-1963 doi: 10.3989/arbor.2011.Extra-3n3136

Por tanto, los sistemas deberían seguir la misma arquitectura de servicios, la misma estructura de mensaje, etc. Para evitar esto, y proporcionar nuevas características: enrutamiento y transformación, SOA se apoya en el bus de servicios de empresa (ESB). Este bus permite que los sistemas sean capaces de entenderse, aun cuando los tipos de datos son diferentes para cada uno y permite enviar la petición al servicio correcto o a la máquina que en ese momento está menos ocupada. Además, proporciona seguridad y monitorización del flujo de información (Figura 12).

Para implementar la arquitectura middleware, es necesario crear un módulo dentro del LMS que permita agregar distintos laboratorios online. Un LMS de código abierto consiste en una base de datos, una estructura lógica de programación (paquetes, módulos, bloques, etc.) y un servidor web. Se puede crear un módulo editando y programando estos elementos.

Moodle permite que un programador pueda crear módulos de actividad y bloques que añadan nuevas funcionalida-

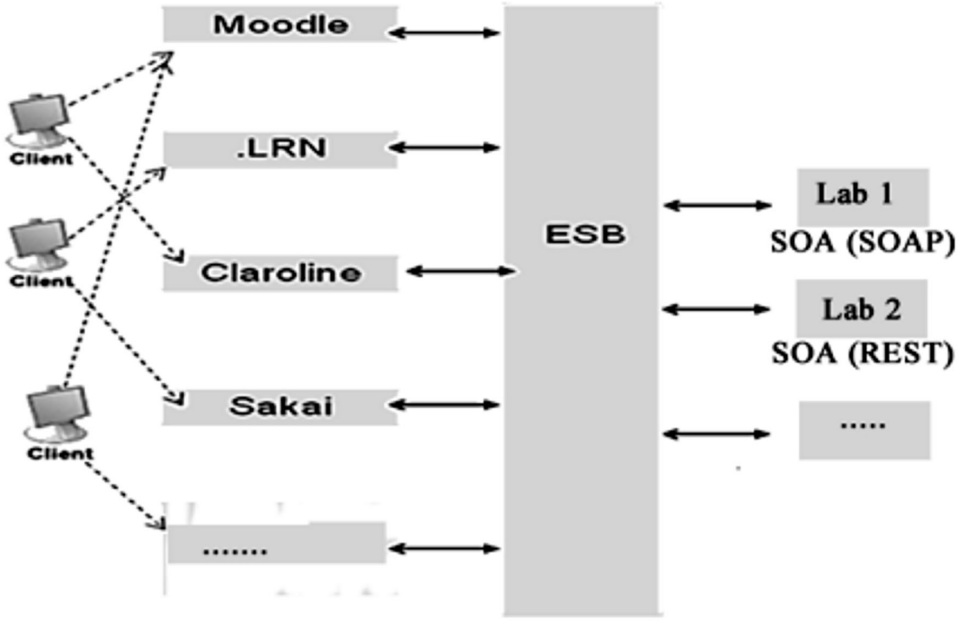

Figura 12. Implementación del bus de servicios de empresa (ESB).

des al sistema. En el departamento se ha desarrollado un módulo para Moodle, de tal forma que el profesor pueda añadir, modificar laboratorios y posteriormente asignarlos a los cursos que ellos crean convenientes. La Figura 13 muestra la estructura del módulo creado con la función de cada fichero.

Una vez instalado el módulo de laboratorios de Moodle. El administrador de Moodle deberá incluir todos los datos de los laboratorios que desea tener en Moodle. Para realizar esta tarea accede a las opciones presentadas en el bloque de administrador de Moodle. Por ejemplo, añadir laboratorio muestra el formulario ya implementado (Figura 14).

Una vez agregado un laboratorio por el administrador, el profesor del curso lo puede implementar en su curso. Las Figuras 15 y 16 muestran un laboratorio (Deusto PLD) agregado por el profesor.

De esta manera, el alumno puede acceder desde el LMS al laboratorio sin tener que autenticase otra vez (Figura 17).

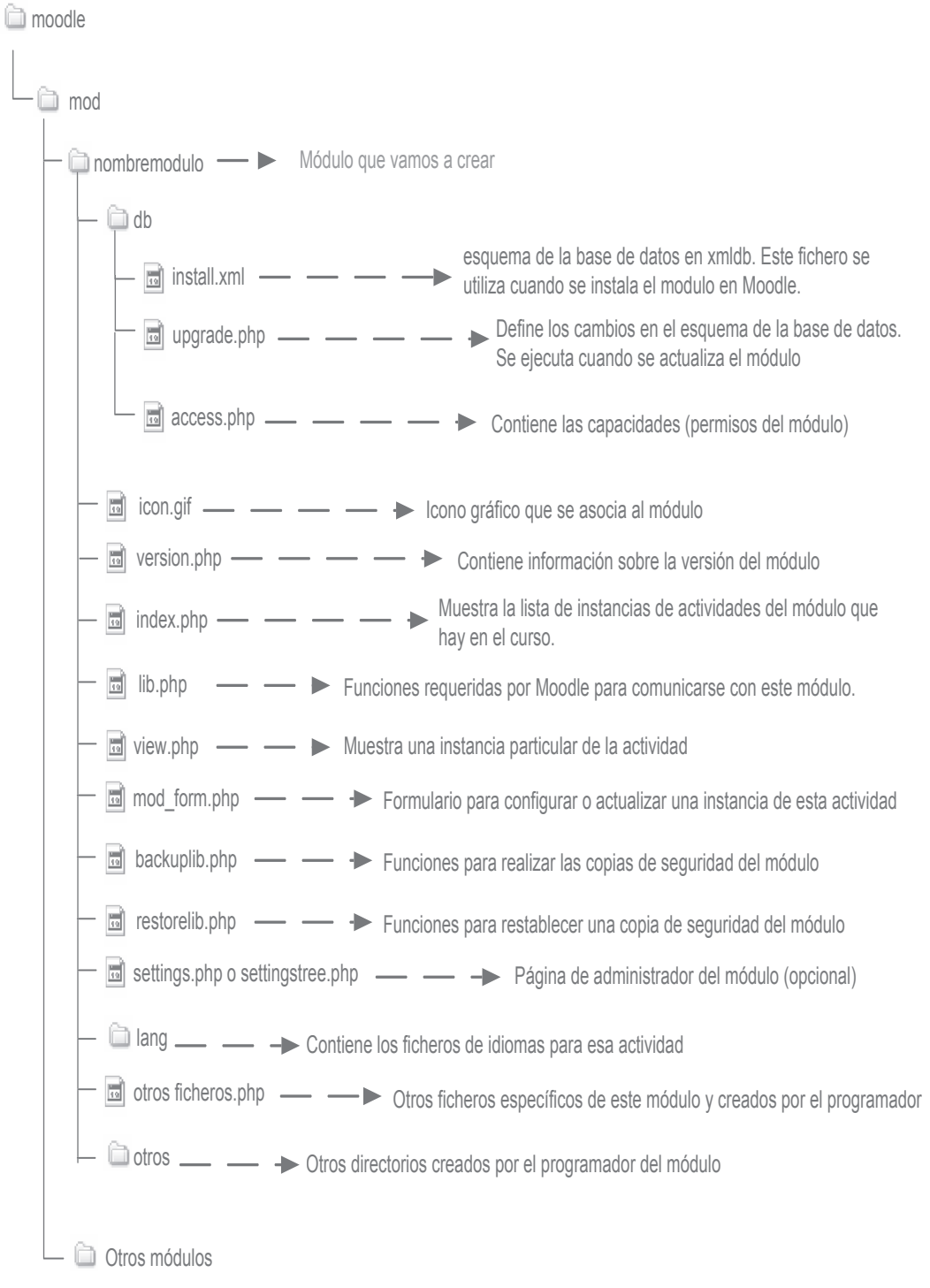

Figura 13. Estructura del módulo creado.

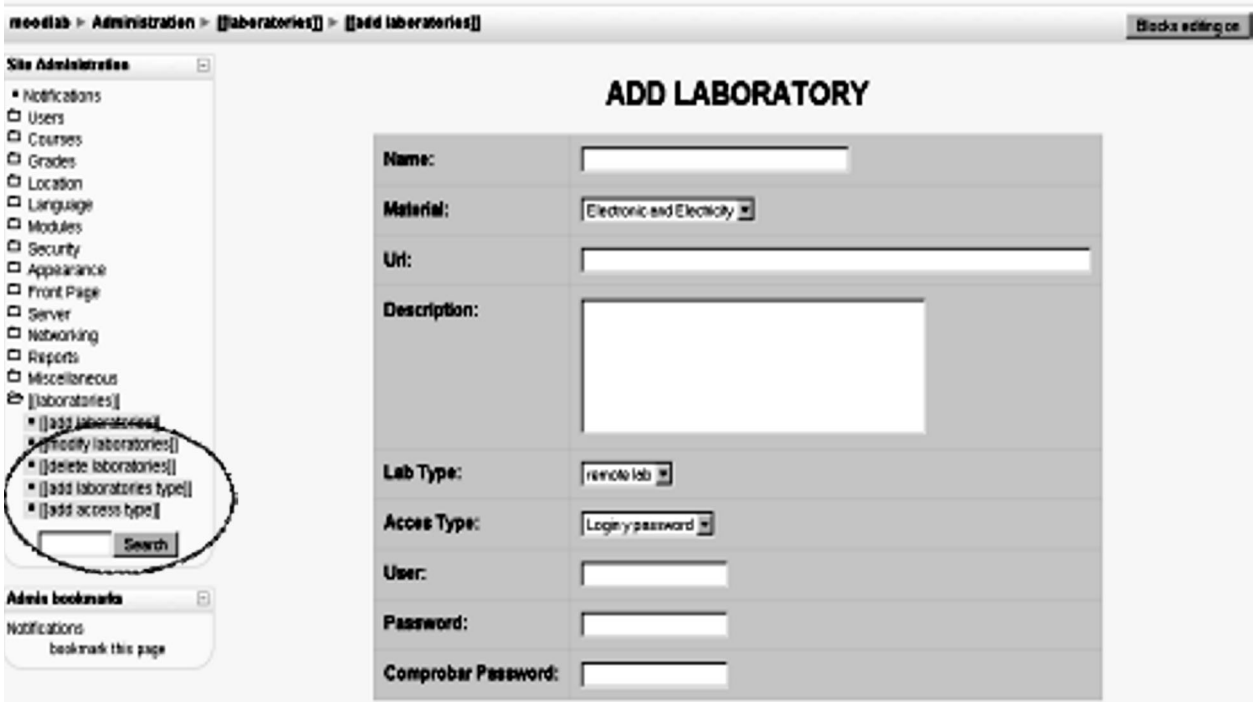

Figura 14. Formulario para añadir un laboratorio en Moodle.

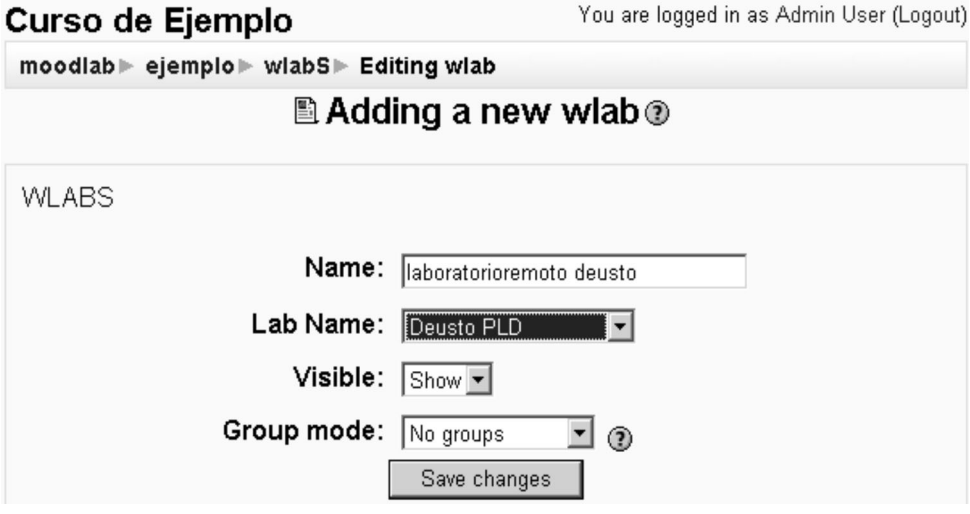

Figura 15. Instancia del laboratorio remoto de la Universidad de Deusto.

doi: 10.3989/arbor.2011.Extra-3n3136 ARBOR Vol. 187 Extra 3 diciembre [2011] 135-151 ISSN: 0210-1963

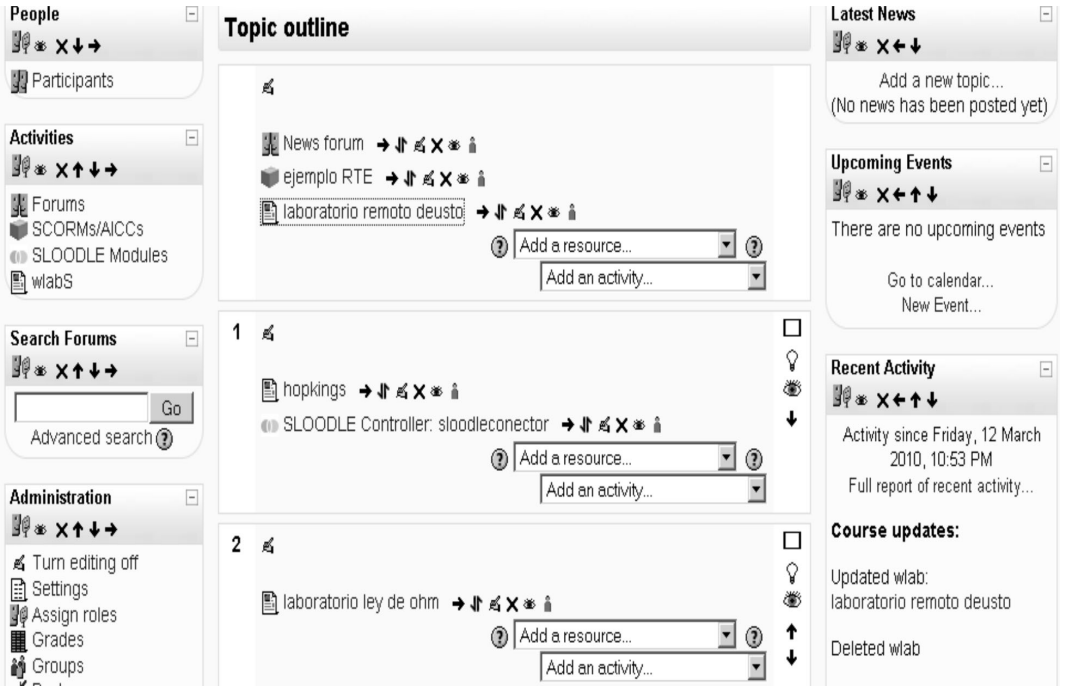

Figura 16. Instancias de laboratorios en un curso Moodle.

Figura 17. Acceso a los experimentos del laboratorio remoto de la Universidad de Deusto.

6. Conclusión

En este artículo se ha presentado una integración de un módulo de comparación de huellas dactilares basado en técnica de minucias en el acceso *(login)* o registro en Moodle. Para ello se realizó una modificación de los archivos vinculados con la autenticación de acceso de Moodle y la tabla de la base de datos de Moodle que posee información del usuario. Por otro lado, se ha presentado una arquitectura middleware capaz de integrar los laboratorios online con los LMS con fin de reutilizar los servicios proporcionados por ambas mediante el uso de módulos creados dentro del LMS y los servicios web. Estas investigaciones marcan el comienzo de nuevas formas de mejorar el nivel de educación a distancia en nuestra universidad, perfilando lo que sería la seguridad de acceso y las prácticas.

Agradecimientos

Los autores quieren agradecer el apoyo del Ministerio Español de Ciencia e Innovación en el proyecto TIN2008-06083-C03/TSI "s-Labs - Integración de Servicios Abiertos para Laboratorios Remotos y Virtuales Distribuidos" y a la CYTED por el proyecto CYTED-508AC0341 "SOLITESOFTWARE LIBRE EN TELEFORMACIÓN". Igualmente a la actividad investigadora de Aprendizaje a la Comunidad de Madid por el apoyo a la red e-Madrid Project, S2009/TIC-1650, "Investigación y Desarrollo de tecnologías para el e-learning en la Comunidad de Madrid".

BIBLIOGRAFÍA

Gil Ortego, Rosario (2010): *Autenticación por Huella Dactilar en Sistemas de Gestión de Aprendizaje y su Análisis Empírico en Estudiantes de Ingeniería,* Tesis Doctoral, UNED (Universidad Nacional de Educación a Distancia).

Harward, V. J.; del Alamo, J. A.; Lerman, S. R.; Bailey, P. y Carpenter, J. *et al.* (2008): "The iLab Shared Architecture: A Web Services Infrastructure to Build Communities of Internet Accessible Laboratories", *Revista de Investigación Educativa,* vol. 26-1, pp. 11-23.

San Cristóbal, Elio (2010): *Metodología, Estructura y Desarrollo de Interfaces Intermedias para la Conexión de Laboratorios Remotos y Virtuales a Plataformas Educativas,* Tesis Doctoral, UNED (Universidad Nacional de Educación a Distancia).