MedivozCaptura. Una Aplicación en Red Segura de Ayuda al Profesional de ORL

V. Osma-Ruiz [a], J.M. Gutiérrez-Arriola [a], J.I. Godino-Llorente [a], N. Sáenz-Lechón [a], R. Fraile [a], J.D. Arias-Londoño [b], E. Hervás-Caballero [a]

[a] *E.U.I.T. Telecomunicación-Universidad Politécnica de Madrid, Cra Valencia Km 7, 28031, Madrid.*

[b] *Grupo de Control y Procesamiento Digital de Señales. Universidad Nacional de Colombia. Manizales*

Corresponding autor: Enrique Hervás Caballero (ehervasca@gmail.com)

Resumen — **MedivozCaptura es una herramienta informática desarrollada para asistir al análisis y detección de patologías vocales. Se basa en el almacenamiento en una base de datos relacional de señales de voz, electroglotogramas (EGG) y vídeo-endoscopias, además de otros datos sobre los pacientes que los especialistas puedan considerar relevantes.**

El presente documento describe el funcionamiento de la aplicación de forma distribuida en red, con la base de datos centralizada, así como la problemática de seguridad y rendimiento que supone la distribución a través de la red o Internet y cómo se solventa en MedivozCaptura.

Index Terms — **Bases de datos distribuidas, seguridad informática, encriptación, patologías vocales, ORL.**

I. Introducción

Hoy en día los sistemas informáticos permiten desarrollar aplicaciones que almacenan y procesan cantidades ingentes de datos. La proliferación de la banda ancha, y la mejora incremental en las velocidades de transmisión tanto en red local como a través de Internet, dotan a los ordenadores de la capacidad necesaria para centralizar estos datos en una misma máquina, independientemente de su localización espacial.

Este tipo de aplicaciones, llamadas comúnmente cliente-servidor, son la base sobre la que se asientan multitud de plataformas existentes hoy en día, desde aplicaciones bancarias hasta retransmisiones televisivas a través de la red.

MedivozCaptura [1] es una plataforma desarrollada específicamente para asistir a los profesionales de ORL a la hora de diagnosticar las múltiples disfunciones que puede padecer el sistema fonador, mediante la captura y almacenamiento de varias señales características de una exploración (vídeo, audio y EGG) y otros datos fundamentales de la anamnesis del paciente. MedivozCaptura usa una base de datos cliente-servidor para habilitar el uso compartido de la información por varios profesionales de ORL a través de una red.

A lo largo de este artículo, se discutirá la problemática que surge de la distribución de datos personales a través de la red, y la utilización de las técnicas más avanzadas para salvaguardar la privacidad e integridad de los datos en el programa MedivozCaptura. Por último se presentarán los resultados obtenidos de diversas pruebas realizadas al sistema y las conclusiones resultantes.

II. Problemática de las Bases de Datos Cliente/Servidor

El marco legal al que están sujetos los sistemas de bases de datos [2], y en general cualquier sistema informático que almacena o transmite datos de índole personal, dispone que es obligatorio adoptar las medidas necesarias para evitar que los datos personales sean manipulados por personas no autorizadas. Esto influye no sólo en la forma de almacenar la información, sino también en el modo de tratarla a la hora de ser transmitida por un medio inseguro, como puede ser Internet.

Idealmente, las comunicaciones seguras abarcan las siguientes propiedades [3]:

- *Confidencialidad*: sólo los agentes que intervienen en el intercambio de información deben ser capaces de comprender el mensaje transmitido.
- *Autenticación y no repudio*: es necesario que se pueda confirmar la identidad de los agentes involucrados.
- *Integridad*: el sistema debe estar protegido frente a alteraciones malintencionadas de la información.
- *Disponibilidad y control de acceso*: la información debe estar disponible siempre y sólo para los usuarios legitimados para el acceso.

Para asegurar estas propiedades es necesario utilizar distintas técnicas, que comprenden desde complejos algoritmos criptográficos hasta las más comunes protecciones físicas.

En concreto, para sistemas de bases de datos distribuidos a través de Internet, estas propiedades deberían abarcar las siguientes tareas [4]:

- *Control de acceso y autenticación*: un buen sistema de autenticación de usuarios impide el acceso a personas ajenas. Además se pueden utilizar distintas reglas para establecer no sólo quién accede a la información sino también a que parte de la información puede acceder. Normalmente se usan sistemas de autenticación mediante claves que solo los usuarios legítimos conocen.

 ISBN: 978-84-693-3389-1

- *Auditoría y monitoreo*: las acciones de auditoría y monitoreo permiten investigar las actividades de los usuarios y detectar problemas y fallos en la seguridad.
- *Proteger las comunicaciones*: en entornos distribuidos potencialmente inseguros como Internet es de especial interés asegurar que la información transmitida a través del medio permanece oculta a terceros. Protocolos como SSL permiten realizar ese intercambio de forma segura.
- *Proteger el fichero de base de datos*: es también importante la protección del propio fichero o ficheros donde se aloja la base de datos. En entornos no distribuidos basta con impedir el acceso físico a la máquina donde se encuentra el fichero, pero esto no basta cuando se trata de una base de datos a la que se accede a través de la red. Son importantes en este aspecto todas las medidas que se puedan tomar, desde *firewalls* hasta la encriptación del fichero de la base de datos (o de los datos que este contenga). Es interesante señalar que hasta el fichero más fortificado estará totalmente desprotegido si no se lleva a cabo correctamente la autenticación de usuarios y la protección de las transmisiones.

III. Técnicas de cifrado

Como parte fundamental de un sistema de bases de datos, la encriptación o cifrado tanto de las comunicaciones de red, como de los datos almacenados, pueden ser factores determinantes para la seguridad.

Actualmente, la criptografía abarca multitud de técnicas, principalmente de carácter matemático, que permiten garantizar el secreto en las comunicaciones telemáticas.

Hay dos clases de algoritmos de cifrado: Algoritmos de clave privada y algoritmos de clave pública.

A. Algoritmos de clave privada

Los algoritmos de clave privada o *algoritmos simétricos* son aquellos que emplean una misma clave tanto para cifrar como para descifrar [5]. Todos los agentes que intervienen en la comunicación deben conocer esa clave.

En la actualidad se usa como estándar el algoritmo AES (*Advanced Encryption Standard*), aunque es también común el 3DES (*Triple Data System Standard*) que fue el estándar anterior.

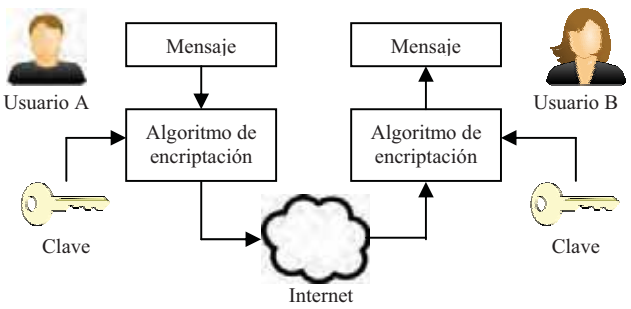

Fig. 1. Esquema de comunicación usando un algoritmo de clave privada.

La Fig. 1 muestra el esquema de una conversación usando clave privada: tanto el usuario A como el B deben conocer, previamente a la comunicación, la clave privada que se usará en el cifrado.

El principal inconveniente de este tipo de cifrado se encuentra en el intercambio de las claves. Ese es el momento crítico en el que una tercera parte malintencionada podría interceptar esa clave. Si el intercambio de claves se realiza de forma segura, los algoritmos simétricos son extremadamente rápidos.

B. Algoritmos de clave pública

En el caso de los algoritmos de clave pública o *asimétricos* se emplean dos claves: una privada que solo posee una persona; y otra pública que se envía al resto de personas que intervienen en la conversación. Una de ellas se usa para cifrar el mensaje, y la otra para descifrarlo. Normalmente, las claves son intercambiables, de forma que si una se usa para cifrar, la otra sirve para descifrar y viceversa, como ocurre con el algoritmo de clave pública más popular a día de hoy, RSA.

Estos algoritmos se usan también como métodos de autentificación, con ayuda de *algoritmos de resumen*, para generar *firmas digitales* de documentos o mensajes [5].

En la Fig. 2 se muestra el envío de un mensaje usando un cifrado de clave pública. El usuario A le envía su clave pública a B, con la que cifrará el mensaje. Sólo A podrá descifrarlo, ya que es el único conocedor de la clave privada.

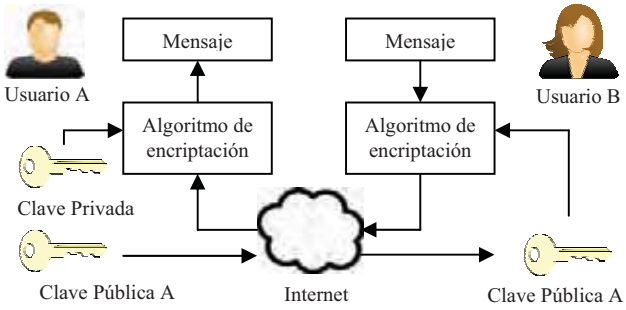

Fig. 2. Esquema de una comunicación usando un algoritmo de clave pública.

Este tipo de algoritmos suelen ser más lentos que los simétricos ya que las operaciones que utilizan son más costosas en términos de rendimiento, por lo que son menos eficientes a la hora de encriptar grandes cantidades de información. Además, tienen el problema de que un usuario malintencionado podría hacerse pasar por otro, y enviar su propia clave pública en lugar de la clave auténtica, sin que nadie se percatase [5].

Debido a esta necesidad de asociar un usuario o máquina con una clave pública de forma inequívoca se utilizan las llamadas infraestructuras de clave pública, donde una entidad certificadora conocida (*autoridad de certificación*) utiliza su clave privada para certificar que un usuario o máquina es quien dice ser.

En la práctica, para realizar intercambios de información de forma segura, se utiliza una mezcla de todas las técnicas. Un

 ISBN: 978-84-693-3389-1

ejemplo de esto es el protocolo SSL (*Secure Socket Layer*) ilustrado en la Fig. 3, que se usa de forma intensiva en aplicaciones distribuidas en Internet. En este protocolo se utilizan técnicas de certificación e infraestructuras de clave pública para autenticar a los usuarios que intervienen y sus claves. Después, mediante un algoritmo de clave pública se intercambia la clave privada (llamada *clave de sesión*) que se usará para cifrar el mensaje con un algoritmo simétrico [3].

IV. Seguridad en MedivozCaptura

MedivozCaptura soporta su uso a través de red local e Internet, siendo la seguridad fundamental debido a que la información que contiene la base de datos puede ser sensible.

Para garantizar dicha seguridad se han implementado tres niveles que los administradores del programa podrán utilizar o no, según la sensibilidad de la información que contengan sus bases de datos y la seguridad de su entorno.

A. Autenticación de usuarios

El primer nivel de seguridad consiste en sólo permitir el acceso a la base de datos a aquellos usuarios que el administrador habilite para ello. MedivozCaptura cuenta con una pequeña aplicación de gestión de usuarios que permite al administrador crear y modificar usuarios, así como sus claves de acceso a la base de datos. La Fig. 4. presenta la interfaz de esta aplicación.

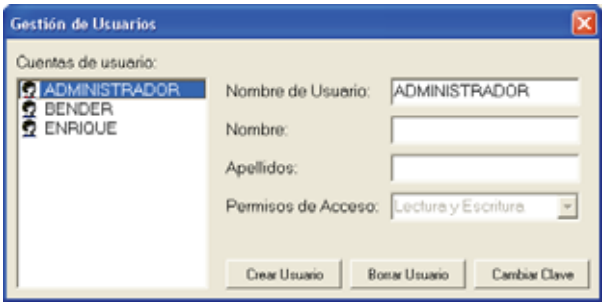

Fig. 4. Pantalla de gestión de usuarios en MedivozCaptura.

Con esta opción activada sólo los usuarios con una cuenta válida que escriban correctamente la contraseña podrán acceder al programa.

B. Encriptación de la base de datos

Para aquellas bases de datos que vayan a funcionar en local, en un ordenador con acceso a Internet, o en un entorno de red inseguro, se puede elegir encriptar todo el contenido de la base de datos. Esta opción asegura que, aunque una persona malintencionada acceda al servidor y obtenga el fichero de la base de datos, no se pueda ver su contenido.

Para la encriptación se utiliza un cifrado AES con una clave de 256 bits de longitud. Este tipo de cifrado es considerado, a día de hoy, invulnerable en la práctica.

El administrador podrá decidir encriptar y desencriptar la base de datos entera. Los usuarios que tengan permiso para entrar pueden ver y modificar la información sin problemas.

C. Cifrado de las comunicaciones con SSL

En bases de datos que se encuentren distribuidas en red o Internet se puede añadir un último nivel de seguridad usando el protocolo SSL para cifrar las comunicaciones.

El administrador de la base de datos podrá configurar el servidor para aceptar conexiones seguras, obteniendo un certificado de clave privada y pública de una autoridad de certificación. Los programas clientes podrán usar el certificado de clave pública del servidor para acceder a los datos de forma segura a través de una red insegura.

Estos tres niveles de seguridad son independientes unos de otros, si bien en algunos casos serán necesarios todos o una mezcla de varios. En un entorno local para un uso unipersonal puede no ser necesario ninguno de ellos. Sin embargo, será recomendable activar tanto encriptación de la base de datos como el uso de SSL si los clientes utilizan el programa a través de Internet. MedivozCaptura permite configurar todos estos parámetros desde la pantalla de configuración que se muestra en la Fig. 5.

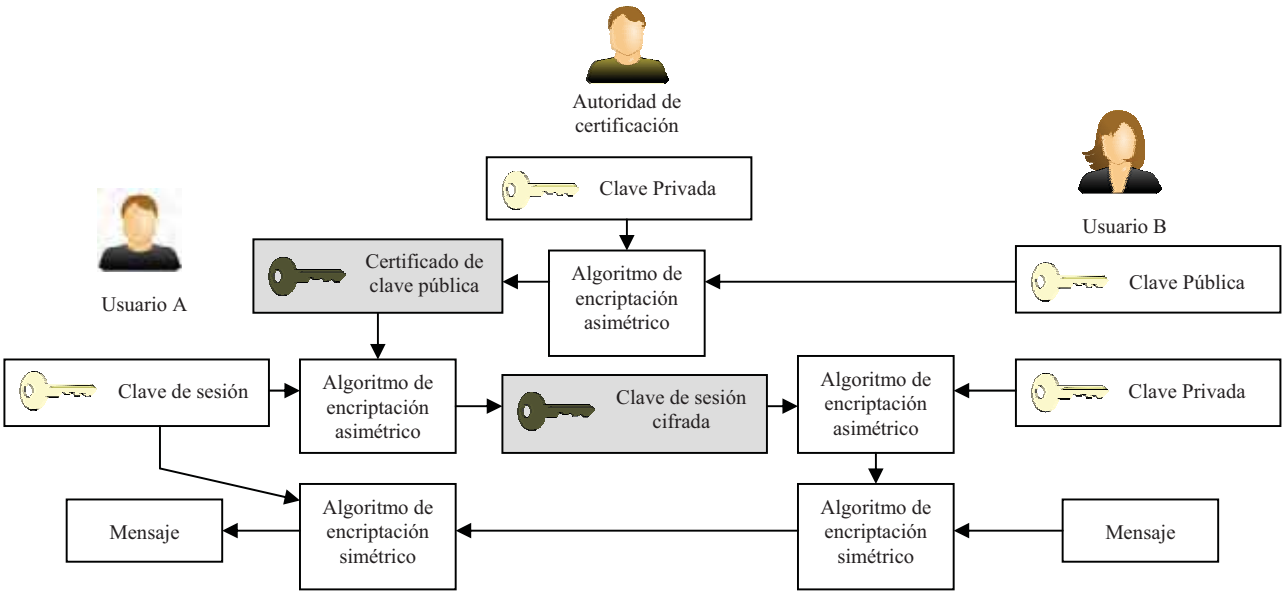

Fig. 3. Esquema del funcionamiento del protocolo SSL para el envío de un mensaje entre dos usuarios que no se conocen entre si.

 ISBN: 978-84-693-3389-1

Fig. 5. Pantalla de configuración de MedivozCaptura.

V. Resultados

Se ha probado el funcionamiento del programa utilizando la encriptación de comunicaciones para guardar y visionar vídeos endoscópicos tanto en un entorno de intranet como en Internet. Los vídeos representan el caso más crítico de funcionamiento ya que suponen el transporte de una gran cantidad de información. Los siguientes resultados promediados se obtuvieron al medir la velocidad de carga y descarga de distintos tamaños de vídeos con la base de datos encriptada tanto en red local (Tabla 1) como a través de Internet (Tabla 2).

	Velocidad en red local 100Mbit/s con protocolo SSL	**Velocidad en red local 100Mbit/s sin protocolo SSL**	**Diferencia relativa**
Carga	27,71 Mbit/s	34,51 Mbit/s	19,7%
Descarga	44,96 Mbit/s	52,60 Mbit/s	14,5%

Tabla 1. Diferencia entre las velocidades de transmisión con y sin SSL en red local.

	Velocidad lograda	**Velocidad contratada**
Carga	150 Kbit/s	165 Kbit/s (cliente)
Descarga	186 Kbit/s	203 Kbit/s (servidor)

Tabla 2. Velocidades de transmisión a través de Internet sin protocolo SSL.

VI. Conclusiones

La encriptación a nivel de base de datos y de las comunicaciones (con SSL) es una solución muy buena para asegurar que el acceso a la base de datos se realiza de forma segura.

Mediante las pruebas realizadas se ha comprobado que la encriptación de los datos para realizar la comunicación cliente-servidor puede entorpecer la velocidad en una red local, sin embargo a través de Internet no supone un lastre significativo ya que la velocidad se ve limitada principalmente por el contrato de subida de datos establecido con el proveedor de servicios de Internet. Esta pérdida de eficiencia en la transmisión es en cualquier caso aceptable si se quiere garantizar la confidencialidad.

Las medidas de seguridad descritas en este documento permiten a MedivozCaptura distribuirse a través de redes inseguras (como Internet) y centralizar los datos de los pacientes. De esta forma especialistas en diferentes localizaciones podrán coordinarse para realizar diagnósticos mejores y más rápidos, sin problemas de seguridad.

VII. Agradecimientos

Este trabajo ha sido financiado por el proyecto TEC2009-14123-C04.

Referencias

[1] Godino Llorente, J.I., "Manual de usuario de MedivozCaptura", pp. 5-6, 2003.

[2] España, Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, 14 de diciembre de 1999, núm 298.

[3] James F. Kurose, Keith W. Ross. "Redes de computadores, un Enfoque Descendente basado en Internet" Pearson Educación, 2003.

[4] Oracle. “Oracle database security guide 10g Release 2 (10.2)”. [En línea]. 2010. Chapter 17, Developing Applications Using Data Encryption. Disponible en Web: http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/apdvncrp.htm#i1007112

[5] Manuel J. Lucena López, "Criptografía y Seguridad en Computadores”. [En línea]. Cuarta Edición. Marzo 2010. Disponible en Web: http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto